

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年9月27日 (27.09.2001)

PCT

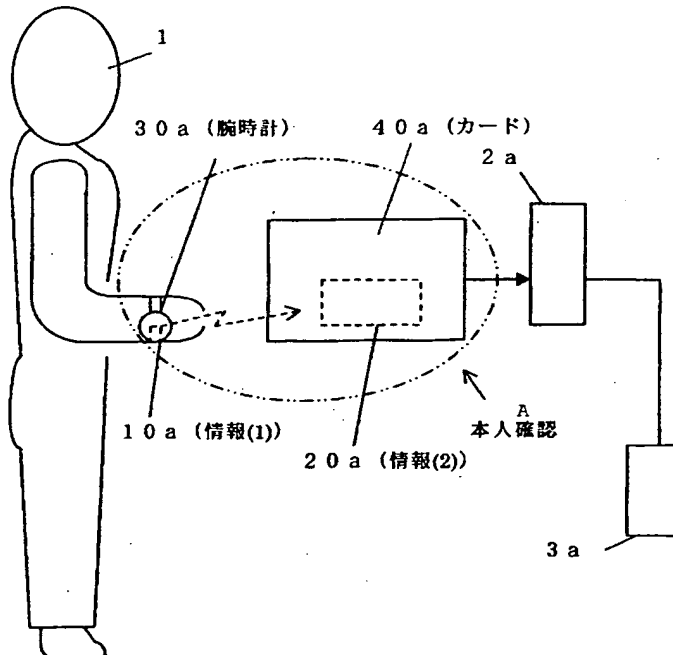
(10) 国際公開番号
WO 01/71516 A1

- (51) 国際特許分類: G06F 15/00, 17/60 (71) 出願人 および
(21) 国際出願番号: PCT/JP01/02329 (72) 発明者: 橋本秀紀 (HASHIMOTO, Hideki) [JP/JP]; 〒107-0052 東京都港区赤坂9丁目5番27号 ルピナス赤坂乃木坂302号.Tokyo (JP).
(22) 国際出願日: 2001年3月23日 (23.03.2001) (72) 発明者; および
(25) 国際出願の言語: 日本語 (75) 発明者/出願人 (米国についてのみ): 深津博一 (FUKATSU, Hirokazu) [JP/JP]; 〒457-0071 愛知県名古屋市中区栄二丁目10番19号 名古屋商工会議所ビル Aichi (JP).
(26) 国際公開の言語: 日本語 (74) 代理人: 岡田英彦, 外(OKADA, Hidehiko et al.); 〒460-0008 愛知県名古屋市中区栄二丁目10番19号 名古屋商工会議所ビル Aichi (JP).
(30) 優先権データ: 特願2000-128648 2000年3月23日 (23.03.2000) JP (81) 指定国 (国内): US.
(71) 出願人 (米国を除く全ての指定国について): 株式会社タイテック (TIETECH CO., LTD.) [JP/JP]; 〒457-0071 愛知県名古屋市中区栄二丁目10番19号 名古屋商工会議所ビル Aichi (JP).

[続葉有]

(54) Title: METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

(54) 発明の名称: 本人確認方法及び本人確認装置



(57) Abstract: A portable user unit (10a) is provided in a portable user device (30a) (such as a wrist watch or glasses), and a user unit (20a) is provided in a user device (40a) (such as a card or portable telephone). Original information is divided to form first information (1) and second information (2). The portable user unit (10a) stores the first information (1), and the user unit (20a) stores the second information (2) and the original information. The portable user unit (10a) transmits the first information (1) stored in itself. The user unit (20a) combines the received information (1) and the second information (2) stored by itself to form third information. If the third information agrees with the original information, the user is authenticated. Upon the authentication, the user device (20a) permits the user to use the user device (40a).

10a... (INFORMATION 1)
20a... (INFORMATION 2)
30a... (WRIST WATCH)
40a... (CARD)
A... PERSONAL IDENTIFICATION

[続葉有]

WO 01/71516 A1



(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約:

ユーザが携帯可能なユーザ携帯機器 (腕時計、眼鏡等) 30 a に設けられるユーザ携帯装置 10 a と、ユーザが使用するユーザ機器 (カードや携帯電話機) 40 a に設けられるユーザ装置 20 a を用いる。原情報を分割して第1情報 (1) と第2情報 (2) を形成する。第1情報 (1) をユーザ携帯装置 10 a に記憶させ、第2情報 (2) と原情報をユーザ装置 20 a に記憶させる。ユーザ携帯装置 10 a は、自身が記憶している第1情報 (1) を送信する。ユーザ装置 20 a は、受信した情報 (1) と自身が記憶している第2情報 (2) を結合して第3情報を形成する。第3情報が原情報と一致する場合に、本人であると確認する。ユーザ装置 20 a は、本人であることを確認すると、ユーザ機器 40 a の使用を許可する。

明 細 書

本人確認方法及び本人確認装置

[技術分野]

本発明は、ユーザ機器を使用するユーザがそのユーザ機器の本来のユーザであることを（本人であること）を確認する本人確認方法及び本人確認装置に関する。特に、認証が必要であるシステムに好適に用いることができる本人確認方法及び本人確認装置に関する。さらには、本人確認装置の生成方法及び生成装置に関する。

[背景技術]

ユーザがサービス会社のサービスを利用する場合、サービス会社は、サービスを利用しようとするユーザが本人であることを確認するために、認証を行っている。

認証方法としては、例えば、暗証番号を用いる方法、サイン用いる方法、印章を用いる方法、IDコードを用いる方法が使用されている。

暗証番号を用いる方法は、例えば、キャッシュカードを用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、現金を引き出す場合、銀行のATM（現金自動支払機）のカード挿入口にキャッシュカードを挿入し、暗証番号を入力する。ATMは、キャッシュカードから読み取ったカード情報（例えば、ID）とユーザが入力した暗証番号を認証センタに送信する。認証センタは、ATMに入力された暗証番号及び読み取ったカード情報と、記憶手段に記憶されているカード情報と暗証番号との対応関係を含むデータベースに基づいて、認証を行う。

サインを用いる方法は、例えば、クレジットカードを用いて商品の代金を支払う場合に用いられる。ユーザは、クレジットカードで代金を支払う場合、商品購入票にサインをする。商品販売者は、商品購入票のサインとクレジットカードに記入されているサインを比較することによって認証を行う。

印章を用いる方法は、例えば、預金通帳を用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、預金通帳を用いて銀行の口座から現金を引き出す場合、現金引出用紙に印鑑を用いて押印する。銀行は、現金引出用紙に押印された印章と予め登録されている印章とを比較することによって認証を行う。

IDコードを用いる方法は、例えば、ユーザが使用するユーザ機器の不正使用を防止する場合等に用いられる。この方法では、ユーザが携帯するタグ（例えば、送受信機能付きのカード）及びユーザが使用するユーザ機器（例えば、携帯電話機）に同じIDコードを記憶させる。タグは、ユーザ機器に接続して使用することもできるが、無線タグとして使用する場合が多い。ユーザ機器は、タグから送信されたIDコードと自己が記憶しているIDコードとを照合し、一致している場合にはユーザ機器の使用制限を解除（例えば、使用許可信号を出力）する。

また、他の認証方法として、各人に固有の生体情報（声紋、指紋、掌紋、網膜パターン、顔を撮像した画像等）を用いる方法が知られている。この認証方法では、生体情報読取装置によってユーザの生体情報を読み取り、読み取った生体情報と予め登録されている生体情報とを照合することによって認証を行うものである。この認証方法は、各人に固有の生体情報を用いるため、認証精度が高い。

暗証番号、サイン、印章やIDコードによって本人確認を行う従来の本人確認方法は、キャッシュカードを使用した人、クレジットカードを使用した人、預金通帳を使用した人、IDコードを記憶したタグを携帯する人が本来のユーザでない場合でも、正しいユーザであると認証してしまうことがある。例えば、ユーザ機器（例えば、キャッシュカード）や印鑑等の盗難、暗証番号、サインやIDコード等の情報盗難や情報漏洩が発生すると、ユーザ機器が不正使用されてしまう。

また、生体情報によって本人確認を行う従来の本人確認方法は、生体情報読取装置（例えば、撮像装置）や生体情報処理装置（例えば、画像処理装置、大容量の記憶装置）等が必要であるため、システム全体のコストが高くなる。また、指に傷がついた場合や眼病になった場合には、指紋や網膜パターンが変化し、認証精度が低下する可能性がある。また、網膜パターンを用いる場合には、目を測定位置に持って行く必要があるため、煩わしさがある。また、指紋を用いる場合に

は、指を指紋読取装置に接触させる必要があるため、きれい好きの人にとっては心理的不快感がある。

[発明の開示]

本発明の目的は、低コストで信頼性の高い本人確認方法及び本人確認装置を提供することである。

本発明の本人確認方法及び本人確認装置は、一つの情報を複数の分割情報に分割し、一部の分割情報をユーザが携帯するユーザ携帯装置に記憶させ、他の分割情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させる。ユーザ携帯装置は、自身が記憶している情報を送信する。ユーザ装置は、受信した情報と自身が記憶している情報とを結合し、所定の情報、例えば、原情報を復元できた場合に、そのユーザ機器の本来のユーザであることを確認し、ユーザ機器の使用を許可する。このように、本発明では、分割した情報を結合する処理だけでよいから、生体情報を用いる場合に比べて安価に構成することができる。また、例えば、カードやIDタグや暗証番号を盗まれても、ユーザ携帯装置及びユーザ装置を盗まれない限り、ユーザ機器が不正使用されることがない。このため、暗証番号、サイン、印章、IDコード等を用いる場合に比べて信頼性が高い。

原情報としては記号、文字、図形、数式等種々の情報を用いることができる。また、原情報を分割する方法も、幾何学的に分割する方法、数式や論理式を用いて分割する方法等種々の方法を用いることができる。この点において、本発明の本人確認方法及び本人確認装置、汎用性がある。

使用するユーザ携帯装置の数は、2以上であってもよい。ユーザ携帯装置が2以上の場合には、使用するユーザ携帯装置の数とユーザ装置の数を加算した数だけ、原情報を分割する。使用する携帯装置の数が多いほど、信頼性は向上するが、結合処理は複雑になる。

本発明を用いた場合でも、ユーザ携帯装置とユーザ装置との間で送受信する情報が漏洩した場合には、ユーザ機器が不正使用される可能性がある。そこで、情報の漏洩を防止する対策を講じる必要がある。本発明の種々の実施例では、種々の情報漏洩防止技術が用いられている。

本発明の好ましい実施例では、送信側に暗号化装置を設け、受信側に復号化装置を設けている。これにより、送信側から受信側の情報を送信する際における、情報の漏洩を防止することができる。

本発明の他の好ましい実施例では、送信側に、原コードを所定の暗号化方法で暗号化した暗号化コードのみを記憶させ、受信側に、復号化方法と原コードを記憶させている。この場合、送信側には暗号化装置が設けられていないため、暗号化コードが漏洩しても、原コードを復号するのは困難である。

本発明の他の好ましい実施例では、暗号化方式として、時間的に変化する暗号化式を用いる暗号化方式を用いている。この実施例では、送信側装置には、任意の時点における暗号化式で原コードを暗号化した暗号化コードのみを記憶させ、受信側装置には、任意の時点における復号化式と原コードを記憶させる。時間的に変化する暗号化式としては、カオス演算式を用いるのが好ましい。カオス演算式を用いて暗号化された暗号化コードが漏洩しても、原コードを復号することはほとんど不可能であるため、信頼性が格段に向上する。

本発明の他の好ましい実施例では、暗号化方式として公開鍵暗号化方式を用いている。この実施例では、ユーザ装置は、ユーザ携帯装置から受信した第1の情報と自身が記憶している第2の情報を、公開鍵を用いて暗号化した暗号化コードを認証センタに送信する。認証センタは、公開鍵に対応する秘密鍵を用いて、受信した暗号化コードを復号化する。そして、第1の情報と第2の情報を結合して原情報を復元できるか否かを判断する。公開鍵暗号化方式を用いれば、公開鍵が漏洩しても暗号化コードを復号することができないため、信頼性が高い。また、1つの受信側に対して1つの公開鍵を割り当てればよいため、鍵の管理が容易である。公開鍵についても、原情報と同様に、例えば、第1公開鍵と第2公開鍵に分割してユーザ携帯装置とユーザ装置に記憶させれば、一層信頼線が高い。

本発明の他の好ましい実施例では、ユーザ機器に、ユーザ装置に記憶されている情報の不正な読み出しを検出した時に、情報の読み出しを禁止する読出禁止装置が設けられている。読出禁止装置としては、例えば、記憶装置を破壊する装置が用いられる。これにより、簡単な構成で、情報が不正に読み取られるのを防止することができる。

また、本発明の他の目的は、本人確認装置を容易に手に入れることができる本人確認装置の生成装置を提供することである。

本発明の好ましい実施例では、暗号装置と、原コード記憶装置と、暗号化コード記憶装置が設けられた回路基板を用意し、任意の時点で回路基板を切断することによって、送信側に設けられる第1の回路基板と、受信側に設けられる第2の回路基板を形成する。この方法を用いれば、暗号化機能を備えた本人確認装置を容易に得ることができる。

本発明の他の好ましい実施例では、ユーザが原情報を入力するとともに、分割方法を指示すると、入力された原情報が指示された分割方法で分割されて第1情報及び第2情報が形成され、第1情報が書き込まれたユーザ携帯装置及び第2情報が書き込まれたユーザ装置が商品排出口から排出される。これにより、ユーザは、容易に、自分の好みにあった本人確認装置を手に入れることができる。

本発明の目的及び利点は、以下に記載されている実施例の記載あるいはクレームを図面を参照しながら読むことによって、よりよく理解することができる。

[図面の簡単な説明]

- 図1は、本発明の本人確認方法の第1実施例を説明する図である。
- 図2は、本発明の本人確認方法における処理手順の例を説明する図である。
- 図3は、本発明の本人確認方法における処理手順の例を説明する図である。
- 図4は、分割情報を結合する例を説明する図である。
- 図5は、分割情報を結合する例を説明する図である。
- 図6は、本発明の本人確認装置の第1実施例のブロック図である。
- 図7は、ユーザ機器の1例を示す図である。
- 図8は、本発明の本人確認方法の第2実施例を説明する図である。
- 図9は、本発明の本人確認方法の第3実施例を説明する図である。
- 図10は、本発明の本人確認方法の第4実施例を説明する図である。
- 図11は、本発明の本人確認装置の第2実施例のブロック図である。
- 図12は、本発明の本人確認装置の第3実施例のブロック図である。
- 図13は、本発明の本人確認装置の第4実施例のブロック図である。

- 図 1 4 は、本発明の本人確認装置の第 5 実施例のブロック図である。
- 図 1 5 は、本発明の本人確認装置の第 6 実施例のブロック図である。
- 図 1 6 は、本発明の本人確認装置の生成装置の一実施例のブロック図である。
- 図 1 7 は、図 1 6 に示す生成装置で生成したユーザ携帯装置及びユーザ装置の例を示す図である。
- 図 1 8 は、本発明の本人確認方法の第 4 実施例を説明する図である。
- 図 1 9 は、本発明の本人確認方法における処理手順の例を説明する図である。
- 図 2 0 は、本発明の本人確認方法における処理手順の例を説明する図である。
- 図 2 1 は、分割情報を結合する例を説明する図である。
- 図 2 2 は、本発明の本人確認装置の第 7 実施例のブロック図である。
- 図 2 3 は、本発明の本人確認装置の生成方法の一実施例を説明する図である。
- 図 2 4 は、本発明の本人確認方法の第 5 実施例を説明する図である。
- 図 2 5 は、本発明の本人確認装置の第 8 実施例のブロック図である。
- 図 2 6 は、本発明の本人確認方法の第 6 実施例を説明する図である。
- 図 2 7 は、本発明の本人確認方法の第 7 実施例を説明する図である。
- 図 2 8 は、本発明の本人確認装置の第 9 実施例のブロック図である。
- 図 2 9 は、分割情報を結合する例を説明する図である。
- 図 3 0 は、分割情報を結合する例を説明する図である。
- 図 3 1 は、本発明の本人確認装置の第 1 0 実施例のブロック図である。
- 図 3 2 は、本発明の本人確認装置の第 1 1 実施例のブロック図である。

[発明を実施するための最良の形態]

以下に、本発明の好ましい実施例を図面を参照して説明する。

本発明に対応する本人確認方法の第 1 実施例を図 1 を用いて説明する。なお、図 1 は、本発明の本人確認方法を用いた認証システムを示している。

例えば、ユーザ 1 が、デビットカード（ユーザ機器）4 0 a を用いて購入品の代金を支払う場合、従来の認証方法では、以下のようにしてユーザ認証が行われる。

まず、ユーザ 1 は、デビットカード 4 0 a を認証端末装置 2 a のカード挿入口

に挿入するとともに、暗証番号を入力手段を用いて入力する。

認証端末装置 2 a は、デビットカード 4 0 a に記憶されているカード情報（ID 等）を読み取る。そして、読み取ったカード情報と、ユーザ 1 が入力した暗証番号を含むユーザ情報を認証センタ 3 a に送信する。

認証センタ 3 a の記憶装置には、暗証番号をカード情報と対応させたデータベースが記憶されている。認証センタ 3 a は、認証端末装置 2 a から送信されたユーザ情報に含まれているカード情報及び暗証番号とデータベースに記憶されている情報とを照合することによって認証を行う。

認証センタ 3 a は、認証が OK であれば、認証 OK 信号を認証端末装置 2 a に送信する。一方、認証が NG であれば、認証 NG 信号を認証端末装置 2 a に送信する。

この認証処理では、前述したように、ユーザ 1 がデビットカード 4 0 a の本来のユーザであることの確認（本人確認）は行われていない。そこで、本実施例では、認証センタ 3 a でユーザ認証処理が行われる前に、本人確認処理（図 1 の二点鎖線で囲んだ部分）が以下のように行われる。

本実施例の本人確認装置は、ユーザ 1 が携帯する腕時計（ユーザ携帯機器） 3 0 a に設けられたユーザ携帯装置 1 0 a と、ユーザが使用するデビットカード（ユーザ機器） 4 0 a に設けられたユーザ装置 2 0 a により構成されている。ユーザ携帯装置 1 0 a とユーザ装置 2 0 a は、例えば、ユーザ認証を行うサービス会社が用意する。ユーザ携帯装置 1 0 a、ユーザ装置 2 0 a を、ユーザ携帯機器 3 0 a、ユーザ機器 4 0 a に取り付ける方法は種々の方法が可能である。例えば、接着剤や接着テープ等を用いて取り付ける方法、ユーザ携帯機器 3 0 a やユーザ機器 4 0 a に内蔵する方法等を用いることができる。

また、本実施例では、ユーザ装置 2 0 a は、本人であることを確認できるまでは、使用禁止信号を出力してデビットカード 4 0 a を使用不能状態とする。すなわち、認証端末装置 2 a がデビットカード 4 0 a のカード情報を読み出すことができないようにする。

ユーザ携帯装置 1 0 a とユーザ装置 2 0 a には、本人確認に必要な情報が記憶されている。例えば、元々一つの情報として認識される情報（原情報）を 2 つに

分割し、第1の分割情報（情報(1)）を、ユーザ携帯機器30aに設けられたユーザ携帯装置（10a）に保有（記憶）させ、第2の分割情報（情報(2)）を、ユーザ機器40aに設けられたユーザ装置20aに保有（記憶）させる。原情報を分割する方法としては、種々の方法を用いることができる。

ユーザ携帯機器30aは、腕時計に限定されず、ユーザ1が携帯可能あるいは携行可能であればよい。例えば、指輪、眼鏡、ベルトのバックル、ブレスレット、ペンダント、イヤリング、ピアス、財布、定期券、免許証等を用いることができる。ユーザ携帯装置10aは、ユーザ携帯機器30aと共に携帯する必要はなく、例えば、ポケットやカバンに入れて携帯してもよい。ユーザ機器40aは、カードに限定されず、本人確認が必要な機器であればよい。例えば、携帯電話機やパソコン等でもよい。ユーザ機器40aは、複数のユーザが共用するものであってもよい。

ユーザ携帯装置10aは、第1の情報(1)をユーザ装置20aに送信する送信手段を備えている。第1の情報(1)を送信する方法としては、無線電波を用いてもよいし、超音波や光（赤外線）を用いてもよい。

ユーザ装置20aは、第1の情報(1)を受信すると、受信した第1の情報(1)と自身が記憶している第2の情報(2)を所定のアルゴリズム（結合方法）で結合して第3の情報(3)を作成（形成）する。そして、第3の情報(3)と原情報を照合することによって本人確認を行う。すなわち、受信した第1の情報(1)と自身が記憶している第2の情報(2)を結合して原情報を再生あるいは復元することができる場合に、本人であることを確認する。前記したように、対応するユーザ携帯装置10aとユーザ装置20aには、同一の原情報から生成された第1の情報(1)と第2の情報(2)を記憶させている。このため、ユーザ装置20aは、第2の情報(2)に対応する第1の情報(1)を受信した場合にだけ、原情報を再生あるいは復元することができる。

図1に示す認証システムでは、デビットカード（ユーザ機器）40aに記憶されているカード情報は、ユーザ装置20aがユーザ1が本人であることを確認した場合にのみ出力される。

例えば、紛失しあるいは盗まれたデビットカード40aを第三者が使用しよう

としても、ユーザ装置 20 a は、デビットカード 40 a の本来のユーザ 1 が携帯しているユーザ携帯装置 10 a から送信される第 1 の情報 (1) を受信することができない。このため、認証センタ 3 a でユーザ認証が行われる前に、デビットカード 40 a に設けられているユーザ装置 20 a の本人確認処理によって不正使用を確実に阻止することができる。

本実施例では、割り符のように、一つの原情報を第 1 の情報 (1) と第 2 の情報 (2) に分割し、第 1 の情報 (1) をユーザ携帯装置 10 a に記憶させ、第 2 の情報 (2) をユーザ装置 20 a に記憶させている。そして、ユーザ装置 20 a は、受信した情報と自身が記憶している情報とを結合して、原情報を形成することができた場合にのみ本人であることを確認する。したがって、生体情報を用いる場合に比して、安価に構成することができる。また、暗証番号やカードを盗まれたり、紛失したりしても、ユーザ携帯機器（ユーザ携帯装置）を盗まれたり、紛失したりしない限り、不正使用の心配がない。また、ユーザ携帯装置 10 a とユーザ装置 20 a には異なる情報を記憶させているので、一方が盗まれたり、紛失しても不正使用の心配がない。したがって、暗証番号、サイン、ID データ等を用いる場合に比べて、信頼性が高い。

なお、本実施例は、ユーザがユーザ機器を使用する際に、ユーザがそのユーザ機器の本当のユーザであるか否かを確認（本人確認）するための方法に関するものである。したがって、ユーザ機器で本人確認処理を行った結果をどのように利用するかは、ユーザ機器の種類やユーザ機器を利用する形態に応じて適宜選択される事項である。例えば、図 1 に示す実施例では、ユーザ装置 20 a は、本人であることを確認すると、デビットカード（ユーザ機器）40 a のカード情報の認証端末装置 2 a への出力を許可する。これにより、デビットカード 40 a のカード情報が認証端末装置 2 a で読み取られる。また、ユーザ 1 は、認証端末装置 2 a の入力手段を用いて暗証番号を入力する。以後は、従来と同様の手順で、認証センタ 3 a でユーザ認証処理（デビットカードの正当性を認証する処理）を行う。

図 2 は、本発明の本人確認方法における処理手順の例を説明する図である。本実施例では、ユーザ装置 20 は、常時本人確認処理を行う。本実施例では、①～

④の手順で本人確認処理が行われる。

①ユーザ携帯装置 10 は、適宜の時期に（例えば、所定の時間間隔で）、自身が記憶している第 1 の情報 (1) を送信する。

②受信待機状態にあるユーザ情報 20 は、情報 (1) を受信する。

③ユーザ装置 20 は、情報 (1) を受信すると、受信した情報 (1) と自身が記憶している第 2 の情報 (2) を所定のアルゴリズムで結合して第 3 の情報 (3) を形成する。

③ユーザ装置 20 は、第 3 の情報 (3) と原情報を照合して、第 3 の情報 (3) と原情報が一致した場合に、ユーザが本人であることを確認する。すなわち、情報 (1) と情報 (2) を結合して原情報を形成することができた場合に、本人であることを確認する。

図 3 は、本発明の本人確認方法における処理手順の他の例を説明する図である。本実施例では、ユーザ装置は、本人確認が必要な場合に本人確認処理を行う。

本実施例では、①～⑥の手順で本人確認処理が行われる。

①ユーザ装置 20 は、本人確認処理を行う必要がある場合（例えば、デビットカードが認証端末装置のカード挿入口に挿入された場合等）に、第 1 の情報 (1) の送信を要求する送信要求信号を送信する。

②受信待機状態にあるユーザ携帯装置 10 は、送信要求信号を受信する。

③ユーザ携帯装置 10 は、送信要求信号を受信すると、自身が記憶している第 1 の情報 (1) を送信する。

④受信待機状態にあるユーザ装置 20 は、情報 (1) を受信する。

⑤ユーザ装置 20 は、情報 (1) を受信すると、受信した情報 (1) と自身が記憶している第 2 の情報 (2) を所定のアルゴリズムで結合して第 3 の情報 (3) を形成する。

⑥ユーザ装置 20 は、第 3 の情報 (3) と原情報を照合し、第 3 の情報 (3) が原情報と一致する場合に、本人であることを確認する。

なお、ユーザ装置 20 は、情報 (1) を受信できない場合、あるいは受信した情報 (1) が正しい第 1 の情報 (1) でない場合には、所定の処理を実行する。例えば、送信要求信号を送信した後、所定時間内に情報 (1) を受信できない場合には、再度送信要求信号を送信する。そして、所定回数送信要求信号を送信しても情報 (1) を受信できない場合には、本人を確認できないと判断し、所定の終了処理を実行

する。例えば、エラーメッセージを認証端末装置に表示させる。

次に、原情報を分割した分割情報を結合する方法を具体的に説明する。

図4に示す例は、原情報[0 1 1 1]を第1の情報(1)[0 0 1 1]と第2の情報(2)[0 1 0 1]に分割している。そして、第1の情報(1)をユーザ携帯装置10に記憶させ、第2の情報(2)と原情報をユーザ装置20に記憶させている。

ユーザ装置20は、情報(1)を受信すると、受信した情報(1)と自身が記憶している第2の情報(2)を所定のアルゴリズムで結合して第3の情報(3)を形成する。本実施例では、受信した情報(1)と第2の情報(2)をOR処理する。受信した情報(1)が正しい第1の情報(1)の場合には、受信した情報(1)と第2の情報(2)をOR処理することによって、原情報[0 1 1 1]が形成される。さらに、第3の情報(3)と原情報とを照合して本人確認を行う。本実施例では、第3の情報(3)が原情報と同じである否かを判断している。例えば、第3の情報(3)と原情報をXOR(排他的論理和)処理する。

分割方法は、図4に示した例に限定されず、分割した第1の情報(1)と第2の情報(2)を所定の論理演算することによって原情報を形成することができればよい。

図5に示す例では、原情報[数字7の図形のビット行列]を、図5に一点鎖線で示す、左右に引いた分割線を境に、上部の第1の情報(1)と下部の第2の情報(2)に分割している。そして、第1の情報(1)をユーザ携帯装置10に記憶させ、第2の情報(2)と原情報をユーザ装置20に記憶させている。

ユーザ装置20は、情報(1)を受信すると、受信した情報(1)と自身が記憶している第2の情報(2)を所定のアルゴリズムで結合して第3の情報(3)を形成する。本実施例では、受信した情報のビット行列と情報(2)のビット行列を結合する。受信した情報(1)が正しい第1の情報(1)である場合には、受信した情報(1)のビット行列と第2の情報(2)のビット行列を結合すると、原情報[数字7の図形のビット行列]が形成される。さらに、第3の情報(3)と原情報を照合して本人確認を行う。本実施例では、第3の情報(3)のビット行列で表される図形が、原情報のビット行列で表される図形と同じであるか否かを判断する。

分割線を引く場所、引き方、分割線の本数等は、適宜選択可能である。また、

原情報を分割する数や分割する位置等は種々変更可能である。例えば、原情報を情報(a1)、情報(a2)、情報(a3)に分割し、情報(a1)と情報(a3)を第1の情報(1)とし、情報(a2)を第2の情報(2)としてもよい。

また、第1の情報(1)及び第2の情報(2)として同じ情報を用いることもできる。この場合、例えば、第2の情報(2) [0 1 1 1] (=第1の情報(1)) と原情報 [0 0 0 0] をユーザ装置20に記憶させる。ユーザ装置20は、受信した情報(1)と自身が記憶している第2の情報(2)をXOR処理して第3の情報(3)を形成する。そして、第3の情報(3)と原情報を照合して本人確認を行う。

受信した情報と自身が保有している情報を結合するアルゴリズムは、原情報を分割する分割方法によって決定される。

次に、本発明の本人確認装置の第1実施例のブロック図を図6に示す。本実施例の本人確認装置は、ユーザ携帯装置10bとユーザ装置20bを有している。

ユーザ携帯装置10bは、信号出力装置11b、変調／復調装置12b、通信装置13bにより構成されている。信号出力装置11bは、例えば、第1の情報(1)を記憶する記憶装置を有し、第1の情報(1)を出力する。第1の情報(1)の形式としては、種々の形式を用いることができる。

変調／復調装置12bは、信号出力装置11bから出力される第1の情報(1)を変調し、通信装置13bを介してユーザ装置20bに送信する。あるいは、変調／復調装置12bは、通信装置13bを介して受信した信号を復調する。そして、復調した信号に送信要求信号が含まれている場合には、第1の情報(1)を変調し、通信装置13bを介して送信する。ユーザ携帯装置10bには、各構成装置に電力を供給する電池が設けられている。

ユーザ装置20bは、通信装置21b、変調／復調装置22b、結合装置23b、信号出力装置24bを有している。変調／復調装置22bは、通信装置21bを介して受信した信号を復調し、結合装置23bに出力する。あるいは、変調／復調装置22bは、送信要求信号を変調し、通信装置21bを介してユーザ携帯装置10bに送信する。そして、その後に通信装置21bを介して受信した信号を復調し、結合装置23bに出力する。

信号出力装置24bは、例えば、第2の情報(2)を記憶する記憶装置を有し、

第2の情報(2)を出力する。結合装置(本人確認装置)23bは、変調／復調装置22bから入力された情報(1)と第2の情報(2)を所定のアルゴリズムで結合して第3の情報(3)を形成する。例えば、割り符を合わせる方法を用いて第1の情報(1)と第2の情報(2)を結合する。さらに、結合装置23b(本人確認装置)は、第3の情報(3)と原情報の照合結果に基づいて本人か否かを確認する。結合装置23bは、信号出力装置24bあるいは変調／復調装置22bと一体に設けてもよい。ユーザ装置20bには、各構成装置に電力を供給する電池が設けられている。

結合装置23bは、例えば、本人が確認されていない時に出力禁止信号を出力する。結合装置23bから出力禁止信号が出力されている場合には、ユーザ機器は使用不能となる。例えば、デビットカードに記憶されているカード情報を認証端末装置で読み取ることができない、あるいは携帯電話を使用することができない。なお、原情報を信号出力装置24bに記憶させてもよい。

ユーザ装置とユーザ機器が別体の場合には、ユーザ装置(結合措置)とユーザ機器との間の信号の伝送は、無線あるいはケーブルを介して行われる。ユーザ装置及びユーザ機器に互いに接続可能な接続端子を設けておけば、接続端子同士を接続するだけでユーザ装置とユーザ機器を接続することができるため、接続作業が容易となる。

ユーザ携帯装置10bの信号出力装置11b、変調／復調装置12b、通信装置13bや、ユーザ装置20bの通信装置21b、変調／復調装置22b、結合装置23b、信号出力装置24bは、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。

本実施例の結合装置23bが、本発明の本人確認装置に対応する。

図7は、ユーザ機器40bの1例の斜視図である。図7に示すユーザ機器40bは、カード状に形成されている。カードの内部には、図6に示した各構成装置21b～24bが設けられている。ユーザ機器40bは、ユーザ携帯装置10bと通信を行う通信機能を備えた通信機器でもある。ユーザ機器40bとしては、磁気カード、ICカード、デビットカード、クレジットカード、キャッシュカード等を用いることができる。例えば、デビットカード、クレジットカードま

たはキャッシュカード等の決済用カードに通信機能を持たせることによって、決済用カードに本人確認機能を持たせることができる。なお、カードは、決済用カードや金融用カードに限定されるものではなく、無線機等の通信機器をカード状に形成したものでよいことは、勿論である。

図 8 は、本発明の本人確認方法の第 2 実施例を説明する図である。本実施例では、携帯電話機 40 c をユーザ機器として用いている。本実施例では、ユーザ装置 20 c は、本人確認処理を行い、その結果に基づいて携帯電話機 40 c の使用を許可するか否かを判断する。例えば、携帯電話機 40 c に設けられているユーザ装置 20 c は、ユーザ携帯装置 10 c から送信される情報 (1) が、自身が記憶している第 2 の情報 (2) に対応する正しい第 1 の情報 (1) である場合にのみ、携帯電話機 40 c の使用を許可する。これにより、携帯電話機 40 c の不正使用を防止することができる。

ユーザ機器 40 c としては、携帯電話機の他に、通信機能を備える各種の機器を用いることができる。例えば、PHS (Personal Handyphone System) 電話機、PDA (Personal Data Assistance、個人用携帯情報端末) 無線機、ETC (Electronic Toll Collection System、ノンストップ自動料金支払システム) 用通信機、ITS (Intelligent Transport Systems、高度道路交通システム) 用の車両通信機、電話通信端末 (例、公衆電話機、FAX 端末)、データ通信端末 (例、パソコン) 等を用いることができる。何をユーザ機器として用いるかは、営業上または設計上の選択事項である。また、携帯電話機 40 c と端末装置 2 c との接続は、通信回路網 4 c を介して行ってもよい。携帯電話機 40 c と端末装置 (例えば、認証端末装置) 2 c との間の接続方法や通信方法は種々の方法を用いることができる。

図 9 は、本発明の本人確認方法の第 3 実施例を説明する図である。本実施例では、ユーザ携帯装置 10 d を IC チップで構成し、指輪 (ユーザ携帯機器) 30 d に取り付けている。勿論、ユーザ携帯装置 10 d は、指輪以外のユーザ携帯機器に取り付けることができる。例えば、ベルトのバックル、ブレスレット、ペンダント、イヤリング、ピアス等に取り付けることができる。本実施例では、ユーザ装置 20 d も IC チップで構成し、無線機 40 d に取り付けている。

ＩＣチップは、集積回路（ＩＣ）をパッケージあるいはモールドし、リード線（外部端子）を備えるＩＣ製品である。ＩＣには、ＬＳＩ（Large Scale Integration）やＶＬＳＩ等も当然に含まれる。回路の集積度は問題ではない。なお、ユーザ携帯装置及びユーザ装置のいずれかをＩＣチップとしてもよいし、両方をＩＣチップとしてもよいことは言うまでもない。さらに、ユーザ装置及びユーザ装置の一部をＩＣチップとしてもよい。

図１０は、本発明の本人確認方法の第４実施例を説明する図である。本実施例では、ユーザ携帯装置１０eを眼鏡（ユーザ携帯機器）３０eに、例えば接着剤を用いて取り付けられている。また、携帯電話機４０eをユーザ機器として用いている。ユーザ携帯装置１０eとユーザ装置２０eとの間の通信は無線で行っている。ユーザ装置２０eの送信装置として携帯電話機４０eの通信装置を用いることもできる。

ユーザ携帯装置１０eは、ＩＣチップでもよい。携帯電話機４０eに代えて、ＩＣカードやＩＣカード製のデビットカード等を用いてもよい。あるいは、携帯電話機能付きのＩＣカード等を用いることもできる。また、ユーザ携帯装置１０eは、眼鏡以外のもの、例えば、ブレスレットやベルト等に取り付けてもよい。ユーザ携帯装置１０eを、ユーザ携帯機器に取り付けず、ユーザ１のポケットやカバンに入れて持ち歩いてもよい。

図１１は、本発明の本人確認装置の第２実施例のブロック図である。本実施例では、ユーザ携帯装置１０fやユーザ装置２０fの構成要素の一部あるいは全部をＩＣチップで構成している。図１１に示す実施例では、ユーザ携帯装置１０fの信号出力装置１１f、変調／復調装置１２f及び通信装置１３fのそれぞれをＩＣチップで構成している。もちろん、これら３つの手段を一つのＩＣチップで構成することもできる。

また、ユーザ装置２０fの信号出力装置２４fをＩＣチップで構成している。

なお、ユーザ装置２０fの通信装置２１f、変調／復調装置２２f、結合装置２３f及び信号出力装置２４fを一つのＩＣチップ２５fで構成することもできる。

図１２は、本発明の本人確認装置の第３実施例のブロック図である。本実施例

では、ユーザ装置 20 g に破壊装置 26 g を設けている。破壊装置 26 g は、例えば、信号出力装置 24 g に記憶されている第 2 の情報 (2) の不正な読み出しを検出した場合に、信号出力装置 24 g から所定の情報が外部に出力されるのを阻止する。

不正な読み出しの検出は、例えば、通信装置 21 g で受信した信号に、正規の読み出し信号以外の読み出し信号が含まれていることにより検出する。信号出力装置 24 g からの信号出力を阻止する方法としては、例えば、信号出力装置 24 g に過電流を流し、信号出力装置 24 g を破壊する方法を用いることができる。あるいは、揮発性の記憶装置に情報等を記憶させている場合には、記憶装置への電源供給を遮断し、記憶装置に記憶されている情報等を消去する方法を用いてもよい。

破壊装置 26 g は、ユーザ装置 20 g が分解されることを検出した場合に、信号出力装置 24 g あるいはユーザ装置 20 g を破壊するものでもよい。

本実施例の破壊装置 26 g が、本発明の読出禁止装置に対応する。

図 13 は、本発明の本人確認装置の第 4 実施例のブロック図である。ユーザ携帯装置 10 h は、信号出力装置 11 h、変調／復調装置 14 h、通信装置 13 h により構成されている。ユーザ装置 20 h は、通信装置 21 h、変調／復調装置 27 h、結合装置 23 h、信号出力装置 24 h により構成されている。本実施例では、ユーザ携帯装置 10 h の変調／復調装置 14 h に、暗号化機能を持たせている（暗号化機能及び復号化機能を持たせる場合もある）。また、ユーザ装置 20 h の変調／復調装置 27 h に、復号化機能を持たせている（暗号化機能及び復号化機能を持たせる場合もある）。

本実施例では、ユーザ携帯装置 10 h は、第 1 の情報 (1) を暗号化して送信する。そして、ユーザ装置 20 h は、受信した信号の暗号を解読して情報 (1) を得る。これにより、セキュリティが一層向上する。なお、ユーザ装置 20 h からユーザ携帯装置 10 h に信号を送信する時にも、信号を暗号化して送信することもできる。

暗号化処理と復号化処理を同じ装置で行ってもよいし、異なる装置で行ってもよい。暗号化方法としては、公知の種々の暗号化方法を用いることができる。

図14は、本発明の本人確認装置の第5実施例のブロック図である。ユーザ携帯装置10iは、信号出力装置11i、変調／復調装置15i、通信装置13iにより構成されている。ユーザ装置20iは、通信装置21i、変調／復調装置28i、結合装置23i、信号出力装置24iにより構成されている。本実施例では、ユーザ携帯装置10iの変調／復調装置15iに、送信信号にランダムノイズ(RN)を挿入する機能を持たせている(RN挿入機能及びRN除去機能を持たせる場合もある)。また、ユーザ装置20iの変調／復調装置28iに、受信した信号からランダムノイズ(RN)を除去する機能を持たせている(RN挿入機能及びRN除去機能を持たせる場合もある)。本実施例では、ユーザ携帯装置10iは、第1の情報(1)にランダムノイズを挿入して送信する。これにより、セキュリティが一層向上する。

ランダムノイズ挿入処理とランダムノイズ除去処理を同じ装置で行ってもよいし、異なる装置で行ってもよい。信号の漏洩を防止する手段としては、ランダムノイズを挿入する方法以外にも公知の種々の方法を用いることができる。

図15は、本発明の本人確認装置の第6実施例のブロック図である。ユーザ携帯装置10jは、信号出力装置11j、変調／復調装置12j、通信装置13jにより構成されている。ユーザ装置20jは、通信装置21j、変調／復調装置22j、結合装置23j、信号出力装置24j、破壊装置26jにより構成されている。

暗号化機能やRNノイズ挿入機能を用いても、本人確認情報である第1の情報(1)や第2の情報(2)が第三者に漏れる可能性はある。

第1の情報(1)あるいは第2の情報(2)が漏れている可能性がある場合には、第1の情報(1)及び第2の情報(2)を交換すればよい。そこで、本実施例では、ユーザ携帯装置10jの信号出力装置11j、ユーザ装置20jの信号出力装置24jを交換可能に構成している。例えば、ユーザ携帯装置10jの信号出力装置11j、変調／復調装置12j及び通信装置13jを一つのICチップ16jで構成している。また、ユーザ装置20jの通信装置21j、変調／復調装置22j、結合装置23j、信号出力装置24j及び破壊装置26jを一つのICチップ25jで構成している。そして、必要な場合には、ユーザ携帯装置10jのIC

チップ16jを交換用のICチップ17jに、また、ユーザ装置20jのICチップ25jを交換用のICチップ27jに交換する。

なお、ICチップの構成は種々変更可能である。例えば、ユーザ携帯装置10jの信号出力装置11j、ユーザ装置20jの信号出力装置24jのみを交換可能に構成することもできる。また、ICチップを交換可能に構成する方法としては、例えば、ピンやソケットにICチップを差し込む構造にする方法等がある。

次に、本発明の本人確認装置を生成する生成装置の一実施例を図16に示す。

本実施例の生成装置は、管理装置50、端末装置61～63により構成されている。管理装置70と各端末装置61～63は、通信回線（例えば、インターネット、電話回線等）70により接続されている。通信回線としては、無線回線を用いることもできる。端末装置61～63は、例えば、コンビニや金融機関等に設置することができる。管理装置50の設置場所は限定されず、また、端末装置61～63が兼用してもよい。

管理装置50は、各端末装置61～63で本人確認装置を生成する際に端末装置61～63の表示手段61bに表示する表示画面の画面情報、入力された原情報を指示された分割方法で分割するプログラム等が記憶された記憶装置を有している。

各端末装置61～63には、CPU等の処理装置61a、表示装置61b、入力装置61c、情報書込装置61d、商品排出装置61e等が設けられている。

入力装置61cとしては、入力キー、記憶媒体に記憶されている情報を読み取る情報読取装置、画像情報を読み取る画像情報読取装置、表示装置の画面を指や入力ペンでタッチするタッチ式入力装置等を用いることができる。

情報書込装置61dは、本人確認装置を構成するユーザ携帯装置の記憶装置及びユーザ装置の記憶装置に情報（第1の情報(1)、第2の情報(2)）を書き込むことができれば接触式、非接触式の種々の情報書込装置を用いることができる。接触式の情報書込装置を用いる場合には、ユーザ携帯装置やユーザ装置の端子を情報書込装置の端子に位置決めする位置決め手段を設けるのが好ましい。

商品排出装置61eは、情報書込装置61dによって情報が書き込まれたユーザ携帯装置及びユーザ装置を商品排出口、例えば、コンビニに設置されている端

末装置に設けられた商品排出口から排出する。

次に、本実施例の生成装置を用いて本人確認装置を生成する処理を説明する。なお、以下では、端末装置 6 1 がコンビニに設置され、ユーザが端末装置 6 1 を用いて本人確認装置を購入する場合について説明する。

また、端末装置 6 1 内に、ユーザ携帯装置及びユーザ装置が、情報書込装置 6 1 d により情報が書込み可能に収納されているものとして説明する。

本人確認装置を購入するユーザは、まず、端末装置 6 1 の表示装置 6 1 b に表示されているメニュー画面で「本人確認装置の販売」を選択する。端末装置 6 1 b の処理装置 6 1 a は、メニュー画面で「本人確認装置の販売」が選択されると、管理装置 5 0 に「本人確認装置購入」信号を送信する。

管理装置 5 0 は、端末装置 6 1 から「本人確認装置購入」信号を受信すると、端末装置 6 1 の表示装置 6 1 b に原情報入力表示画面を表示させるための入力画面情報を端末装置 6 1 に送信する。これにより、端末装置 6 1 の処理装置 6 1 a は、原情報入力画面を表示装置 6 1 b に表示する。

ユーザは、表示装置 6 1 b に原情報入力画面が表示されている状態で、まず、入力装置 6 1 c を用いて原情報を入力する。原情報を入力する方法としては、種々の方法を用いることが可能である。例えば、①表示装置 6 1 b に表示されている原情報入力画面に入力ペンを用いて好みの数字、文字、記号、図形等を描く方法、②記録媒体に記憶されている原情報を情報読取装置により読み取る方法、③紙等に印刷されている画像を画像情報読取装置で読み取る方法等を用いることができる。図 1 6 に示す実施例では、入力ペンを用いて原情報入力画面に「E」を描いた状態を示している。

次に、入力装置 6 1 c を用いて、原情報を分割するための分割方法を指示する。原情報を分割する分割方法としては、種々の方法が可能である。例えば、原情報を分割線で分割する方法や、所定の論理式で分割する方法等を用いることができる。図 1 6 に示す実施例では、入力ペンを用いて原情報入力画面に分割線（図 1 6 の 2 点鎖線）を引いた状態を示している。

ユーザは、原情報を入力し、分割方法（この場合、分割線）を指示した後、分割処理を指示する。例えば、原情報入力画面に表示されている「入力終了」部を

選択する。端末装置 6 1 は、分割処理が指示されると、原情報及び分割方法を管理装置 5 0 に送信する。例えば、原情報入力画面上の原情報のビットパターン、表示画面上に引かれた分割線の表示画面上における位置情報を送信する。

管理装置 5 0 は、端末装置 6 1 の処理装置 6 1 a から送信された原情報及び分割方法を受信すると、入力された原情報を指示された分割方法で分割して、第 1 の情報 (1) 及び第 2 の情報 (2) を形成する。この場合、管理装置 5 0 は、分割線の位置情報を受信することにより、分割線で分割する分割方法が指示されたものと判断する。図 1 6 に示す実施例では、原情報「E」を分割線で分割し、分割線で分割された「E」の左側の部分の情報を第 1 情報 (1) (図 1 7 参照) とし、分割線で分割された「E」の右側の部分の情報を第 2 情報 (2) (図 1 7 参照) とする。そして、形成した第 1 情報 (1) 及び第 2 情報 (2) を端末装置 6 1 に送信する。

端末装置 6 1 の処理装置 6 1 a は、第 1 情報 (1) 及び第 2 情報 (2) を受信すると、情報書込装置 6 1 d に第 1 情報 (1)、第 2 情報 (2) 及び原情報 (この場合、入力画面上に描かれた「E」の情報) を出力する。

情報書込装置 6 1 d は、第 1 情報 (1) をユーザ携帯装置 1 0 の記憶装置に書き込み、第 2 情報 (2) 及び原情報をユーザ装置 2 0 の記憶装置に書き込む。

商品排出装置 6 1 e は、第 1 情報が書き込まれたユーザ携帯装置 1 0、第 2 情報及び原情報が書き込まれたユーザ装置 2 0 を商品排出口から排出する。

ユーザは、商品排出口から排出されたユーザ形態装置 1 0 及びユーザ装置 2 0 を受け取る。

商品排出口から排出するユーザ携帯装置 1 0 及びユーザ装置 2 0 は、ユーザが使用する用途に応じて種々の形態のものが用いられる。例えば、ユーザ携帯装置 1 0 をユーザ携帯機器 (腕時計、眼鏡、ベルト、イヤリング、キーホルダ等) に取りつけて使用する場合には、微小な (例えば、数 mm^2 程度) 四角形状の IC チップで形成し、取付手段によりユーザ携帯機器に取り付ける。取付手段としては、例えば、IC チップの一方側の面に塗布された接着剤、クリップ、接着テープ等を用いることができる。ユーザ装置 2 0 をユーザ機器 (例えば、携帯電話機) 4 0 に接続して使用する場合には、例えば、ユーザ機器 (携帯電話機) 4 0 に設けられているデータ入出力端子 (接続端子) 4 9 に接続可能な端子 2 9 が設け

られているユーザ装置 20 を用いる。

勿論、ユーザ携帯装置 10 が一体に組み込まれているユーザ携帯機器（腕時計、眼鏡、ベルト、イヤリング、キーホルダ等）や、ユーザ装置 20 が一体に組み込まれているユーザ機器（キャッシュカード、デビットカード、携帯電話機、携帯端末等）を販売することも可能である。この場合には、ユーザ携帯装置 10 をユーザ携帯機器に取り付ける作業や、ユーザ装置 20 をユーザ機器に取り付ける作業が不要である。また、一体に形成されているため、取扱いが容易である。

ユーザ携帯装置 10 やユーザ装置 20 の形態は、端末装置毎に予め定めておいてもよいし、ユーザが本人確認装置を得る際に選択できるようにしてもよい。

なお、ユーザが本人確認装置の購入代金を支払うステップを設けてもよい。購入代金の支払方法は適宜選択可能である。

図 17 に、本実施例の生成装置により生成されたユーザ携帯装置 10 及びユーザ装置 20 を示す。ユーザ携帯装置 10 には、原情報「E」を分割して形成された第 1 情報 (1) が記憶されている。ユーザ装置 20 には、原情報「E」を分割して形成された第 2 情報 (2) 及び原情報「E」が記憶されている。

図 17 に示すユーザ携帯装置 10 は、ユーザ機器に接着剤等によって取り付けで使用したり、あるいはそのまま財布、ハンドバックやポケット等に入れて携帯するものである。

また、図 17 に示すユーザ装置 20 は、携帯電話機 40 のデータ入出力端子（接続端子）49 に接続可能な接続端子 29 が設けられている。この本人確認装置を使用する時には、ユーザ装置 20 の接続端子 29 と携帯電話機 40 のデータ入力端子 49 を接続する。これにより、ユーザ装置 20 の処理装置（図示省略）と携帯電話機 40 の処理装置 45 との間の信号の伝送が可能となる。携帯電話機 40 の処理装置 45 は、例えば、ユーザ装置 20 から出力禁止信号が出力されている時は、携帯電話機 40 の使用を禁止する。

なお、図 16 に示す実施例では、管理装置と端末装置により構成したが、端末装置自体に管理装置の機能を持たせることもできる。この場合には、端末装置単独で生成装置を構成することができる。また、表示装置 61b に表示された原情報を、表示装置 61b で指示された分割線に基づいて分割したが、原情報の入力

方法及び分割線の指示方法はこれに限定されない。さらに、分割線の数や引き方も図16に示した方法に限定されない。また、原情報及び分割線を手で入力したが、原情報や分割線を予め複数用意しておき、その中から選択するようにしてもよい。この場合、原情報及び分割線の一方を手で入力するように構成すれば、分割情報が同一になる可能性は少ない。また、分割線に基づいて原情報を分割したが、原情報を分割する方法はこれに限定されない。また、商品排出装置を用いたが、商品排出装置は省略することもできる。また、端末装置61～63の設置場所は適宜変更可能である。また、ユーザ携帯装置やユーザ装置に情報を書き込む時の方法（手順）は、実施例で説明した方法に限定されず、種々の方法を用いることができる。

以上の実施例では、原情報を2つに分割したが、3以上に分割することもできる。原情報を3つに分割した場合の本人確認方法の実施例を図18に示す。

本実施例では、本人確認処理（図18の二点鎖線で囲んだ部分）が以下のように行われる。

本実施例では、本人確認装置は、第1ユーザ携帯装置110a、第2ユーザ携帯装置（120a及びユーザ装置130aにより構成されている。第1ユーザ携帯装置110a及び第2ユーザ携帯装置120aは、ユーザ1が携帯する腕時計（第1ユーザ携帯機器9140a及び眼鏡（第2ユーザ携帯機器）150aに設けられている。ユーザ装置130aは、ユーザが使用するデビットカード（ユーザ機器）160aに設けられている。本実施例では、ユーザ装置130aは、例えば、本人であることを確認できるまでは、使用禁止信号を出力してデビットカード160aを使用不能状態とする。

元々一つの情報として認識される原情報を3つに分割し、第1の分割情報(1)を第1のユーザ携帯装置110aに、第2の分割情報(2)を第2のユーザ携帯装置120aに、第3の分割情報(3)をユーザ装置130aに記憶させている。

なお、第1及び第2ユーザ携帯機器140a及び150aは同じユーザ携帯機器を用いてもよい。また、第1及び第2のユーザ携帯装置110a及び120aは、ユーザ携帯機器140a及び150aと共に携帯する必要はなく、例えば、財布、カバンやポケットに入れて携帯してもよい。

第1及び第2ユーザ携帯装置110a及び120aは、第1の情報(1)及び第2の情報(2)を送信する送信手段を備えている。

ユーザ装置130aは、情報(1)及び情報(2)を受信すると、受信した情報(1)及び情報(2)と自身が記憶している第3の情報(3)を所定のアルゴリズムで結合して第4の情報(4)を形成する。そして、第4の情報(4)と原情報を照合することによって本人確認を行う。すなわち、受信した第1情報(1)と第2情報(2)と自身が記憶している情報(3)を結合して原情報を再生あるいは復元することができた場合に、本人であることを確認する。

図19は、原情報を3つに分割した場合の本人確認方法における処理手順の例を説明する図である。本実施例では、ユーザ装置130は、常時本人確認処理を行う。本実施例では、①～⑤の手順で本人確認処理が行われる。

①ユーザ携帯装置110は、適宜の時期に第1情報(1)を送信する。

②ユーザ携帯装置120は、適宜の時期に第2情報(2)を送信する。

ここで、ユーザ携帯装置110及び120が同時に情報を送信すると、双方の情報が干渉してユーザ装置130で情報を正確に受信できなくなる可能性がある。そこで、ユーザ携帯装置110の送信時期とユーザ携帯装置120の送信時期が重ならないように設定するのが好ましい。例えば、ユーザ携帯装置110とユーザ携帯装置120が送信する時期を予め設定しておく。

③受信待機状態にあるユーザ装置130は、情報(1)及び情報(2)を受信する。

④ユーザ装置130は、受信した情報(1)及び情報(2)と自身が記憶している第3の情報(3)を所定のアルゴリズムで結合して第4の情報(4)を形成する。

⑤ユーザ装置130は、第4の情報(4)が原情報と一致した場合に、ユーザが本人であることを確認する。

図20は、原情報を3つに分割した場合の本人確認方法における処理手順の他の例を説明する図である。本実施例では、ユーザ装置130は、本人確認が必要な場合に本人確認処理を行う。本実施例では、①～⑤の手順で本人確認処理が行われる。

①ユーザ装置130は、本人確認処理を行う必要がある場合に、送信要求信号を送信する。

②受信待機状態にあるユーザ携帯装置 110 は、送信要求信号を受信すると、自身が記憶している第 1 の情報 (1) を送信する。

③受信待機状態にあるユーザ携帯装置 120 は、送信要求信号を受信すると、自身が記憶している第 2 の情報 (2) を送信する。

ここで、ユーザ携帯装置 110 及び 120 が同時に情報を送信すると、双方の情報が干渉してユーザ装置 130 で情報を正確に受信できなくなる可能性がある。そこで、ユーザ携帯装置 110 の送信時期とユーザ携帯装置 120 の送信時期が重ならないように設定するのが好ましい。例えば、送信要求信号を受信してからそれぞれ異なる待機時間が経過した後に情報を送信するように設定する。

④受信待機状態にあるユーザ装置 130 は、受信した情報 (1) 及び情報 (2) と自身が記憶している第 3 の情報 (3) を所定のアルゴリズムで結合して第 4 の情報 (4) を形成する。

⑤ユーザ装置 130 は、第 4 の情報 (4) が原情報と一致する場合に、本人であることを確認する。

次に、原情報を 3 つに分割した分割情報を結合する例を図 21 により具体的に説明する。

本実施例では、原情報 [数字 7 の図形のビット行列] を、左右に引いた 2 本の分割線 (1) 及び分割線 (2) を境に、上部の第 1 の情報 (1) と、中央の第 2 の情報 (2) と、下部の第 3 の情報 (3) に分割している。そして、第 1 の情報 (1) をユーザ携帯装置 110 に記憶させ、第 2 の情報 (2) をユーザ携帯装置 120 に記憶させ、第 3 の情報 (3) 及び原情報をユーザ装置 130 に記憶させる。

ユーザ装置 130 は、受信した情報 (1) 及び (3)、自身が記憶している第 3 の情報 (3) を所定のアルゴリズムで結合して第 4 の情報 (4) を形成する。本実施例では、各情報のビット行列を結合する。そして、第 4 の情報 (4) と原情報を照合して本人確認を行う。

本発明の本人確認装置の第 7 実施例のブロック図を図 22 に示す。本実施例では、第 1 のユーザ携帯装置 110 b、第 2 のユーザ携帯装置 120 b 及びユーザ装置 130 b により構成されている。

第 1 のユーザ携帯装置 110 b は、信号出力装置 111 b、変調／復調装置 1

1 2 b、通信装置 1 1 3 bにより構成されている。第 2 のユーザ携帯装置 1 2 0 bは、信号出力装置 1 2 1 b、変調／復調装置 1 2 2 b、通信装置 1 2 3 bにより構成されている。信号出力装置 1 1 1 b、1 2 1 bは、それぞれ第 1 の情報 (1)、第 2 の情報 (2) を記憶している。

ユーザ装置 1 3 0 bは、通信装置 1 3 1 b、変調／復調装置 1 3 2 b、結合装置 1 3 3 b、信号出力装置 1 3 4 bにより構成されている。信号出力装置 1 3 4 bは、第 3 の情報 (3) 及び原情報を記憶する。結合装置 1 3 3 bは、受信した情報 (1) 及び第 2 情報 (2) と、自身が記憶している第 3 の情報 (3) を所定のアルゴリズムで結合して第 4 の情報 (4) を形成する。そして、第 4 の情報 (4) と原情報の照合結果に基づいて本人か否かを確認する。

以上の実施例では、原情報を 3 つに分割したが、原情報を 4 つ以上に分割することもできる。すなわち、本発明は、以下のように構成することができる。①原情報を分割して、N 個 (N は 2 以上の整数) の分割情報を形成する。②第 1 分割情報～第 (N-1) 分割情報をそれぞれ第 1 ユーザ携帯装置～第 (N-1) ユーザ携帯装置に記憶させるとともに、第 N 分割情報をユーザ装置に記憶させる。③ユーザ装置 (本人確認手段) は、受信した情報と自身が記憶している情報を所定のアルゴリズムで結合し、原情報を形成することができた場合にユーザがそのユーザ機器の本来のユーザであることを確認する。

次に、暗号化機能を備えた本人確認装置の生成方法の一実施例を、図 2 3 を参照して説明する。

図 2 3 に示すように、まず、暗号装置 8 1、原コード記憶装置 8 2、暗号化コード記憶装置 8 3、接続線 8 4 が設けられた回路基板 X を用意する。

暗号装置 8 1 は、暗号化式を用いて原コードを暗号化し、あるいは暗号化された暗号化コードを復号化式を用いて復号化するものである。原コードとしては、種々の情報を用いることができる。本実施例では、暗号装置 8 1 は、カオスジェネレータで生成されたカオス演算式を用いて暗号化式及び復号化式を決定し、暗号化式を用いて原コードを暗号化し、あるいは暗号化された暗号化コードを復号化式を用いて復号化する。カオスジェネレータは、時間的に変化するカオス演算式を発生する。ある時点でのカオス演算式は、原理的には初期値によって決定さ

れる。このカオス演算式を用いた暗号化式によって原コードを暗号化し暗号化コードは、カオス演算式の初期値がわからない場合には、ほとんど復号化することができない。カオスジェネレータは公知であるため、詳しい説明は省略する。

原コード記憶装置 8 2 は、各時点における原コード（時間に対して一定の原コードを用いる場合と、時間に対して変化する原コードを用いる場合がある）、その時点に暗号装置 8 1 で生成された復号化式を記憶する。

暗号化コード記憶装置 8 3 は、各時点における、暗号装置 8 1 で生成された暗号化式で原コードを暗号化した暗号化コードを記憶する。

暗号装置 8 1 と暗号化コード記憶装置 8 3 との間は、接続線 8 4 で接続されている。接続線 8 4 が切断されると、暗号化コード記憶装置 8 3 への暗号化コードの記憶は停止される。すなわち、暗号化コード記憶装置 8 3 には、回路基板 X が切断された時点における暗号装置 8 1 の暗号化式によって原コードを暗号化した暗号化コードが記憶保持される。

回路基板 X には、回路基板 X を切断しやすいように、適当な個所に切断部が形成されている。本実施例では、回路基板 X の中央部に切り込み形成されている。回路基板 X には、切断部の両側に、第 1 回路基板 X (1) 及び第 2 回路基板 X (2) が形成されている。

第 1 回路基板 X (1) には、暗号装置 8 1 及び原コード記憶装置 8 2 が設けられている。第 1 回路基板 X (1) には、情報の送受信をおこなうための、変調／復調装置や通信装置が設けられている。また、本人確認処理を実行するための本人確認装置が設けられている。暗号装置 8 1 が本人確認装置を兼用してもよい。第 1 回路基板 X (1) には、暗号装置 8 1 等に電力を供給する電池が設けられている。

第 2 回路基板 X (2) には、暗号化コード記憶装置 8 3 が設けられている。第 2 回路基板 X (2) には、情報の送受信をおこなうための、変調／復調装置や通信装置が設けられている。第 2 回路基板 X (2) には、各装置に電力を供給する電池が設けられている。

本人確認装置を生成する場合には、任意の時間に、図 2 3 に示す回路基板 X を切断部 X の部分で切断する。これにより、回路基板 X は、第 1 回路基板 X (1) と第 2 回路基板に分割される。同時に、通信線 8 4 が切断され、暗号装置 8 1 と暗

号化コード記憶装置 8 3 との接続が切断される。これにより、暗号化コード記憶装置 8 3 には、切断時点における暗号装置 8 1 の暗号化式で原コードを暗号化した暗号化コードが記憶保持される。

また、切断時点における原コード、切断時点における暗号装置 8 1 の復号化式が原コード記憶装置 8 2 に記憶保持される。

このようにして形成された第 1 回路基板 X (1) 及び第 2 回路基板 X (2) は、一対の割符部材、すなわち本人確認装置を構成する。この場合、第 1 回路基板 X (1) を受信側の割符部材（ユーザ装置）として用い、第 2 回路基板 X (2) を送信側の割符部材（ユーザ携帯装置）として用いる。

例えば、第 2 回路基板 X (2) を有するユーザ携帯装置は、暗号化コード記憶装置 8 3 に記憶されている暗号化コードを送信する。一方、第 1 回路基板 X (1) を有する受信側のユーザ装置は、受信した暗号化コードを、原コード記憶装置 8 2 に記憶されている復号化式で復号化する。そして、復号化したコードが、原コード記憶装置 8 2 に記憶されている原コードと一致した場合、自己と組になる割符部材であると判断する。すなわち、本人であることを確認する。

なお、信号の送受信を行うための通信装置や本人確認装置は、第 1 回路基板 X (1) 及び第 2 回路基板 X (2) に設けてもよいし、第 1 回路基板 X (1) 及び第 2 回路基板 X (2) を有するユーザ装置やユーザ携帯装置に設けてもよい。

図 2 4 は、以上のようにして生成した本人確認装置を用いて認証システムを構成した図を示している。

図 2 4 に示す実施例では、本人確認装置は、腕時計（ユーザ携帯機器）30k に設けられたユーザ携帯装置 10k と、デビットカード（ユーザ機器）40k に設けられたユーザ装置 20k により構成されている。ユーザ携帯装置 10k には第 2 回路基板 X (2) が設けられ、ユーザ装置 20k には第 1 回路基板 X (1) が設けられている。

ユーザ携帯装置 10k は、記憶装置 8 3 に記憶されている暗号化コードを送信する。ユーザ装置 20k は、暗号化コードを受信すると、受信した暗号化コードを、原コード記憶装置 8 2 に記憶されている復号化式で復号化する。そして、復号化したコードが、原コード記憶装置 8 2 に記憶されている原コードと一致した

場合に、本人であることを確認する。これにより、デビットカード 40 k の使用が可能となる。

次に、図 2 4 に示した本人確認装置の例を図 2 5 に示す。

ユーザ携帯装置 10 m は、信号出力装置 11 m、変調／復調装置 12 m、通信装置 13 m により構成されている。信号出力装置 11 m は、暗号化コード記憶装置 83 を有し、暗号化コードを出力する。

ユーザ装置 20 m は、通信装置 21 m、変調／復調装置 22 m、本人確認装置 23 m、信号出力装置 24 m を有している。信号出力装置 24 m は、原コード記憶装置 82 を有し、原コード及び復号化式を出力する。本人確認手段 23 m は、受信した暗号化コードを、信号出力装置 24 m から出力される復号化式で復号化する。そして、復号化したコードを、信号出力装置 24 m から出力される原コードと照合して本人確認を行う。

図 2 4 に示した本人確認装置の他の例を図 2 6 に示す。図 2 6 に示す実施例は、携帯電話機 40 n をユーザ機器として用いている。また、ユーザ携帯装置 10 n をポケットに入れて持ち運んでいる。

以上の実施例では、携帯装置で本人確認処理を行ったが、例えば認証センタで本人確認処理を行うこともできる。認証センタ等で本人確認処理を行う認証装置を用いた認証システムを図 2 7 に示す。

本実施例では、公開鍵暗号化方式を用いて情報を送信することにより、情報の漏洩を防止している。公開鍵暗号化方式は、公知の暗号化方式であるため詳しい説明は省略するが、公開鍵と秘密鍵を用いる。公開鍵を用いて暗号化された情報は、公開鍵に対応する秘密鍵以外では復号化することができない。情報送信側は、情報受信側の公開鍵を用いて送信情報を暗号化して送信する。情報受信側では、受信した情報を自己の秘密鍵を用いて復号化する。この公開鍵暗号化方式を用いると、共通鍵暗号化方式のように秘密鍵を相手に知らせる必要がないため、秘密鍵が漏洩する恐れが少ない。また、情報受信側は、一つの公開鍵は用いることができるため、共通鍵暗号化方式に比べて鍵の数が少なくすむ。

本実施例の本人確認装置は、腕時計（ユーザ携帯機器）30 p に設けられたユーザ携帯装置 10 p と、デビットカード（ユーザ機器）40 p に設けられたユー

ザ装置 20 p と、認証センタ 160 p とにより構成されている。

本実施例では、他の実施例と同様に、原情報を分割して第 1 の情報 (1) と第 2 の情報 (2) を形成し、第 1 の情報 (1) をユーザ携帯装置 10 p に記憶させ、第 2 の情報 (2) をユーザ装置 20 p に記憶させる。認証センタ 160 p の記憶手段 (図示省略) には、各ユーザ機器 40 p に設けられるユーザ装置 20 p に記憶されている情報 (2) の基となった原情報と、各ユーザ装置 20 p で用いている公開鍵 P K に対応する秘密鍵 S K を各ユーザ装置 20 p (ユーザ機器 40 p) に対応させた記憶しているデータベースが記憶されている。

ユーザ携帯装置 10 p は、自身が記憶している第 1 の情報 (1) を送信する。ユーザ装置 20 p は、受信した情報 (1) と自身が記憶している第 2 の情報 (2) を公開鍵を用いて暗号化し、認証端末装置 150 p を介して認証センタ 160 p に送信する。認証センタ 160 p は、ユーザ装置 20 p から送信された情報を受信すると、記憶手段に記憶されているデータベースに基づいて、ユーザ装置 20 p に対応する秘密鍵 S K を検索する。検索した秘密鍵 S K を用いて、受信した情報を復号化する。すなわち、ユーザ装置 20 p が受信した情報 (1) と、ユーザ装置 20 p が記憶している情報 (2) を抽出する。そして、復号化した情報 (1) と情報 (2) を結合して第 3 の情報 (3) を形成し、第 3 の情報と原情報を照合して本人確認を行う。認証センタ 160 p は、本人を確認できた場合には、例えば、認証 OK 信号を認証端末装置 150 p に送信する。これにより、認証端末装置 150 p は、デビットカード 40 p の使用を許可する。例えば、デビットカード 40 p のカード情報の読み取りや暗証番号の入力を可能とする、あるいは代金の支払を可能とする。

ユーザ装置 20 p から認証センタ 160 p に情報を送信する方法は、種々の方法が可能である。例えば、ユーザ機器が非接触式の通信装置 (無線通信装置) を備えていないデビットカードである場合には、ユーザ機器と認証端末装置 150 p との接続端子、認証端末装置 150 p、通信回線 170 を介して認証センタ 160 p に至る伝送ルート R 1 を介して情報を認証センタ 160 p に送信する。ユーザ機器が無線通信装置を有する携帯電話機である場合には、無線通信回線、通信回線 170 を介して認証センタ 160 p に至る伝送ルート R 2 を介して情報を

認証センタ 160 p 送信する。ユーザ装置 20 p が無線通信装置を有している場合には、無線通信回線、通信回線 170 を介して、ユーザ装置 20 p から認証センタ 160 p に直接送信してもよい。

次に、公開鍵暗号化方式を用いた本人確認装置の例を図 28 に示す。

ユーザ携帯装置 10 q は、信号出力装置 11 q、変調／復調装置 12 q、通信装置 13 q により構成されている。信号出力装置 11 q は、第 1 の情報 (1) を記憶する記憶装置を有している。

ユーザ装置 20 q は、通信装置 21 q、変調／復調装置 22 q、暗号化装置 23 q、信号出力装置 24 q を有している。信号出力装置 24 q は、第 2 の情報 (2) と、情報を暗号化するとき用いる鍵（本実施例では、公開鍵 PK）を記憶する記憶装置を有している。暗号化装置 23 q は、受信した情報 (1) と、信号出力装置 24 q から出力される情報 (2) を、信号出力装置 24 q から出力される公開鍵 PK を用いて暗号化し、通信装置（図示省略）を介して外部（認証センタ 160 p）に送信する。認証センタ 160 p に情報を送信する通信装置は、通信装置 21 q を兼用してもよいし、ユーザ機器に設けられている通信装置を用いてもよい。

認証センタ 160 p は、ユーザ装置 20 q から受信した情報を、当該情報を暗号化した公開鍵に対応する秘密鍵を用いて復号化する。そして、復号化した情報 (1) と情報 (2) を結合して原情報を形成することができた場合に、ユーザ 1 がそのユーザ機器の本来のユーザであることを確認する。

ユーザ装置 20 q に公開鍵を記憶させる方法としては、種々の方法が可能である。例えば、予めユーザ装置 20 q の信号出力装置 24 q に記憶させておく方法を用いる。あるいは、本人確認処理を行う必要がある時または任意の時期に、認証センタ 160 p からユーザ装置 20 q に送信する方法を用いる。あるいは、本人確認処理を行う必要がある時または任意の時期に、認証センタ 160 p が公開鍵を登録した第三者の認証機関から送信する方法を用いる。

次に、原情報を分割した分割情報を結合する方法の例を具体的に説明する。

図 29 に示す例では、原情報 [0 1 1 1] を第 1 の情報 (1) [0 0 1 1] と第 2 の情報 (2) [0 1 0 1] に分割している。そして、第 1 の情報 (1) をユーザ携帯

装置 10 に記憶させ、第 2 の情報 (2) をユーザ装置 20 に記憶させている。原情報は、認証センタ 60 の記憶装置に記憶させている。

ユーザ装置 20 は、受信した情報 (1) と、自身が記憶している情報 (2) を、所定の公開鍵 PK で暗号化 (『PK (情報 (1))』、『PK (情報 (2))』) して、認証センタ 60 に送信する。

認証センタ 60 は、ユーザ装置 20 から受信した情報 (『PK (情報 (1))』、『PK (情報 (2))』) を、ユーザ装置 20 で使用した公開鍵 PK に対応する秘密鍵 SK で復号化 (『SK [PK (情報 (1))]』、『SK [PK (情報 (2))]』) して情報 (1) 及び情報 (2) を得る。

さらに、復号化した情報 (1) 及び情報 (2) を所定のアルゴリズムで結合して第 3 の情報 (3) を形成する。次いで、情報 (3) と原情報とを照合して本人確認を行う。

図 30 に示す例では、原情報 [数字 7 の図形のビット行列] を、図 30 で左右に引いた分割線を境に、上部の第 1 の情報 (1) と下部の第 2 の情報 (2) に分割する。そして、第 1 の情報 (1) をユーザ携帯装置 10 に記憶させ、第 2 の情報 (2) をユーザ装置 20 に記憶させる。原情報は、認証センタ 60 a の記憶装置に記憶させる。

ユーザ装置 20 は、受信した情報 (1) と、自身が記憶している情報 (2) を、所定の公開鍵 PK で暗号化 (『PK (情報 (1))』、『PK (情報 (2))』) して、認証センタ 160 に送信する。

認証センタ 160 は、ユーザ装置 20 から受信した情報 (『PK (情報 (1))』、『PK (情報 (2))』) を、ユーザ装置 20 で使用した公開鍵 PK に対応する秘密鍵 SK を用いて復号化 (『SK [PK (情報 (1))]』、『SK [PK (情報 (2))]』) して情報 (1) 及び情報 (2) を得る。

さらに、復号化した情報 (1) 及び情報 (2) を所定のアルゴリズムで結合して情報 (3) を形成する。さらに、情報 (3) と原情報を照合して本人確認を行う。

上記実施例では、ユーザ装置に公開鍵を記憶させたが、公開鍵も分割してユーザ携帯装置とユーザ装置に記憶させることにより、より信頼性を高めることができる。公開鍵を分割して記憶させる実施例を図 31 に示す。

図 31 に示す実施例では、原情報を分割して形成した第 1 の情報 (1) をユーザ

携帯装置 10 r に記憶させ、第 2 の情報 (2) をユーザ装置 20 r に記憶させている。さらに、所定の公開鍵 PK を分割して第 1 の公開鍵 PK (1) 及び第 2 の公開鍵 PK (2) を形成する。そして、第 1 の公開鍵 PK (1) をユーザ携帯装置 10 r に記憶させ、第 2 の公開鍵 PK (2) をユーザ装置 20 r に記憶させる。

ユーザ携帯装置 10 r は、第 1 の情報 (1) 及び第 1 の公開鍵 (1) を送信する。

ユーザ装置 20 r の暗号化装置 23 r は、受信した公開鍵 PK (1) と自身が記憶している公開鍵 PK (2) を所定のアルゴリズムで結合して公開鍵 PK を形成する。所定のアルゴリズムは、公開鍵 PK の分割方法によって決定される。そして、受信した情報 (1) と自身が記憶している情報 (2) を、公開鍵 PK (1) 及び PK (2) を結合して形成した公開鍵 PK を用いて暗号化し、認証センタ 160 p に送信する。

認証センタ 160 p は、受信した情報をユーザ装置 20 r が用いている公開鍵 PK に対応する秘密鍵 SK を用いて復号化する。そして、復号化した情報と原情報を照合して本人確認を行う。

本実施例では、情報 (1) 及び公開鍵 PK (1) の双方が正しくないと、本人であると確認されないため、信頼性が高くなる。

ユーザ機器として携帯電話機を用い、公開鍵暗号化方式を用いて情報を送信する本人確認装置を図 32 に示す。

本実施例では、ユーザ携帯装置 10 s は、ユーザ 1 の胸ポケットに入れて携帯している。また、ユーザ装置 20 s は、携帯電話機 40 s (ユーザ機器) に取り付けられている。ユーザ装置 20 s に、携帯電話機 40 s のデータ入出力端子と接続可能な接続端子を設けると、ユーザ装置 20 s と携帯電話機 40 s との接続作業が容易となる。

以上の説明では、ユーザ携帯装置とユーザ装置との間の情報の送受信を非接触で行ったが、接触させた状態で情報の送受信をおこなうこともできる。例えば、ユーザ携帯機器としての磁気的あるいは電氣的な ID カード、ID カードタグ、携帯電話機を、ユーザ機器としてのパソコンのカード挿入口に差込みあるいはケーブルで接続しても良い。この場合、ID カードあるいは携帯電話機から第 1 情報をパソコンに送信する。パソコンは、受信した情報と自己が保有する情報とを

結合して原情報を形成することができた場合には、パソコンの使用を許可する。あるいは、逆に、パソコンをユーザ携帯装置、ＩＤカードや携帯電話機をユーザ機器として用いることもできる。

本発明は、以下に記載する効果を有する。

本発明は、生体情報、暗証番号、サイン（署名）、印章あるいはＩＤコード等を用いるのではなく、割り符のような、元々は一つの情報または信号を分割した情報を用いている。そして、各分割情報を、ユーザが携帯するユーザ携帯装置とユーザが使用するユーザ機器に設けられるユーザ装置にそれぞれ記憶させ、ユーザ携帯装置とユーザ装置が記憶している情報を結合した情報に基づいて本人確認を行っている。このような情報は、生体情報のように変動することがない。また、通信手段や各情報の結合手段等は、ＩＣチップ等によって簡単に、安価に構成することができる。したがって、精度が高く、かつ低コストで本人確認を行うことができる。

また、本発明では、ユーザ携帯装置が記憶している情報とユーザ装置が記憶している情報が結合されて原情報が復元されない限り、本人確認が行われない。このため、暗証番号、カードやＩＤタグ等を盗まれても不正使用の心配がない。つまり、ユーザ装置及びユーザ携帯装置を落としたり、盗まれたりしない限り、不正使用の恐れはない。ユーザ携帯装置をＩＣチップで構成すれば、ユーザが携帯可能な多くの部材（例えば、指輪やメガネ）に取り付けることができる。この場合、ユーザ携帯装置を、ユーザが自分で決めた部材に取り付けることができるので、ユーザ携帯機器が盗まれる恐れもほとんどない。万一、情報が漏れている恐れがある場合には、ユーザ携帯装置及びユーザ装置の所定のＩＣチップを新たなチップに交換すればよい。

以上のように、本発明を用いることにより、不特定多数のユーザに対して、簡単、低コスト、高信頼性、高セキュリティで本人確認処理を行うことができる。

本発明は、前記した実施例の構成に限定されることなく、本発明の要旨を変更しない範囲で種々の変更、追加、削除が可能である。例えば、ユーザ装置とユーザ機器との組付け形態、ユーザ携帯装置とユーザ携帯機器との組付け形態は、一体構成あるいは別体構成等種々変更可能である。

請 求 の 範 囲

1. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、

原情報を第1情報と第2情報に分割し、第1情報をユーザが携帯するユーザ携帯装置に記憶させるとともに、第2情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させるステップと、

ユーザ携帯装置から第1情報を送信するステップと、

ユーザ装置で情報を受信するステップと、

ユーザ装置で受信した情報とユーザ装置が記憶している第2情報を結合し、原情報を形成することができた場合に本人であることを確認するステップと、を備えることを特徴とする本人確認方法。

2. 請求項1に記載の本人確認方法であって、

ユーザ携帯装置から第1情報を送信するステップでは、第1情報を暗号化して送信し、

ユーザ装置で情報を受信するステップでは、受信した情報を復号化する、ことを特徴とする本人確認方法。

3. 請求項1に記載の本人確認方法であって、

ユーザ携帯装置から第1情報を送信するステップでは、第1情報にランダムノイズを挿入し、

ユーザ装置で情報を受信するステップでは、受信した情報からランダムノイズを除去する、

ことを特徴とする本人確認方法。

4. 請求項1に記載の本人確認方法であって、

ユーザ携帯装置から第1情報を送信するステップでは、第1情報を無線で送信する、

ことを特徴とする本人確認方法。

5. 請求項1に記載の本人確認方法であって、更に、

ユーザ装置から情報送信要求信号を送信するステップを備え、

ユーザ携帯装置から第1情報を送信するステップでは、ユーザ携帯装置が情報

送信要求信号を受信した時に第1情報を送信する、
ことを特徴とする本人確認方法。

6. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置とを備え、

ユーザ携帯装置は、原情報を分割して形成した第1情報と第2情報のうちの第1情報を記憶する第1記憶装置と、第1記憶装置に記憶されている第1情報を変調する変調装置と、第1通信装置とを有し、

ユーザ装置は、原情報を分割して得た第1情報と第2情報のうち第2情報を記憶する第2記憶装置と、第2通信装置と、第2通信装置で受信した情報を復調する復調装置と、復調装置で復調した情報と第2記憶装置に記憶している第2情報を結合して原情報を形成することができた場合に本人であることを確認する本人確認装置とを有する、

ことを特徴とする本人確認装置。

7. 請求項6に記載の本人確認装置であって、

ユーザ携帯装置は、所定時間毎に第1情報を送信する、

ことを特徴とする本人確認装置。

8. 請求項6に記載の本人確認装置であって、

ユーザ装置は、本人確認が必要な時に情報送信要求信号を送信し、

ユーザ携帯装置は、情報送信要求信号を受信した時に第1情報を送信する、

ことを特徴とする本人確認装置。

9. 請求項6に記載の本人確認装置であって、

ユーザ携帯装置は、第1情報を暗号化する暗号化装置を有し、

ユーザ装置は、受信した情報を復号化する復号化装置を有する、

特徴とする本人確認装置。

10. 請求項6に記載の本人確認装置であって、

ユーザ携帯装置は、第1情報にランダムノイズを挿入するランダムノイズ挿入装置を有し、

ユーザ装置は、受信した情報からランダムノイズを除去するランダムノイズ除去装置を有する、

ことを特徴とする本人確認装置。

11. 請求項6に記載の本人確認装置であって、

ユーザ装置は、更に、不正に第2情報が読み出されることを検出した時に第2記憶装置に記憶されている第2情報の読み出しを禁止する読出禁止装置を有する、

ことを特徴とする本人確認装置。

12. 請求項11に記載の本人確認装置であって、読出禁止装置は第2記憶装置を破壊する、本人確認装置。

13. 請求項6に記載の本人確認装置であって、ユーザ携帯装置及びユーザ装置の少なくとも一方はICチップを含んでいる、ことを特徴とする本人確認装置。

14. 請求項13に記載の本人確認装置であって、ICチップが交換可能に設けられている、ことを特徴とする本人確認装置。

15. 請求項6に記載の本人確認装置であって、ユーザ機器がカード状部材である、ことを特徴とする本人確認装置。

16. 請求項6に記載の本人確認装置であって、ユーザ機器が決済用カードであり、本人確認装置は、本人であることを確認した場合に決済用カードに記憶されているカード情報の読み出しを許可する、ことを特徴とする本人確認装置。

17. 請求項6に記載の本人確認装置であって、ユーザ機器が通信機である、ことを特徴とする本人確認装置。

18. 請求項17に記載の本人確認装置であって、本人確認装置は、本人であることを確認した場合に通信機の使用を許可する、ことを特徴とする本人確認装置。

19. 請求項6に記載の本人確認装置の生成装置であって、ユーザ装置には、ユーザ機器の接続端子と接続可能な接続端子が設けられている、ことを特徴とする本人確認装置。

20. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯する N 個 (N は3以上の整数) のユーザ携帯装置と、
ユーザが使用するユーザ機器に設けられるユーザ装置とを備え、
第1～第($N-1$) のユーザ携帯装置は、それぞれ第1～第 N 記憶装置と、第1～第($N-1$) 記憶装置に記憶されている情報を送信する第1～第($N-1$) 通信装置とを有し、

ユーザ装置は、第 N 記憶装置と、第 N 通信装置と本人確認装置を備え、
第1～第($N-1$) 記憶装置は、原情報を分割して形成した第1～第 N の情報の中の第1～($N-1$) 情報を記憶し、

第 N 記憶装置は、原情報を分割して形成した第1～第 N の情報の中の第 N の情報を記憶し、本人確認装置は、通信装置で受信した情報と第 N 記憶装置に記憶されている情報を結合し、原情報を形成することができた場合に本人であることを確認する、

ことを特徴とする本人確認装置。

21. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、

原情報を第1情報と第2情報に分割し、第1情報をユーザが携帯するユーザ携帯装置に記憶させ、第2情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させるステップと、

ユーザ携帯装置から第1情報を送信するステップと、

ユーザ装置で第1情報を受信するステップと、

ユーザ装置で受信した第1情報とユーザ装置が記憶している第2情報をユーザ装置から認証センタに送信するステップと、

認証センタで、ユーザ装置から送信された第1情報及び第2情報を受信するステップと、

認証センタで受信した第1情報と第2情報を結合して、原情報を作成することができた場合に本人であることを確認するステップと、

を備えることを特徴とする本人確認方法。

22. 請求項21に記載の本人確認方法であって、

ユーザ装置で受信した第1情報とユーザ装置が記憶している第2情報をユーザ

装置から認証センタに送信するステップでは、ユーザ装置で受信した第1情報とユーザ装置が記憶している第2情報を公開鍵で暗号化して認証センタに送信し、

認証センタで第1情報及び第2情報を受信するステップでは、受信した情報を、ユーザ装置で用いている公開鍵に対応する秘密鍵を用いて復号化する、ことを特徴とする本人確認方法。

23. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、

原情報を第1情報と第2情報に分割し、第1情報をユーザが携帯するユーザ携帯装置に記憶させ、第2情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させるステップと、

公開鍵を第1公開鍵と第2公開鍵に分割し、第1公開鍵をユーザ携帯装置に記憶させ、第2公開鍵をユーザ装置に記憶させるステップと、

ユーザ携帯装置から第1情報及び第1公開鍵を送信するステップと、

ユーザ装置で第1情報及び第1公開鍵を受信するステップと、

ユーザ装置で受信した第1情報とユーザ装置が記憶している第2情報を、ユーザ装置で受信した第1公開鍵とユーザ装置が保有している第2公開鍵を結合した公開鍵を用いて暗号化して認証センタに送信するステップと、

認証センタで暗号化情報を受信するステップと、

認証センタで受信した暗号化情報を、ユーザ装置で用いられている公開鍵に対応する秘密鍵を用いて第1情報と第2情報を復号化し、復号化した第1情報と第2情報を結合し、原情報を作成することができた場合に本人であることを確認するステップと、

を備えることを特徴とする本人確認方法。

24. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置と、

認証センタとを備え、

ユーザ携帯装置は、原情報を分割して得た第1情報と第2情報のうちの第1情

報を記憶する第1記憶装置と、第1記憶装置に記憶されている第1情報を送信する第1通信装置とを有し、

ユーザ装置は、原情報を分割して得た第1情報と第2情報のうちの第2情報を記憶する第2記憶装置と、第2通信装置と、第2通信装置で受信した第1情報と第2記憶装置に記憶している第2情報を認証センタに送信する第3通信装置とを有し、

認証センタは、ユーザ装置から送信された第1情報と第2情報を結合して、原情報を形成することができた場合に本人であることを確認する本人確認装置を有する、

ことを特徴とする本人確認装置。

25. 請求項24に記載の本人確認装置であって、

ユーザ携帯装置は、第2通信装置で受信した第1情報と第2記憶装置に記憶されている第2情報を暗号化する暗号化装置を有し、

認証センタは、ユーザ装置から送信された暗号化情報を復号化する復号化装置を有する、

ことを特徴とする本人確認装置。

26. 請求項25に記載の本人確認装置であって、

暗号化装置は、公開鍵を用いて暗号化を行い、

復号化装置は、公開鍵に対応する秘密鍵を用いて復号化を行う、

ことを特徴とする本人確認装置。

27. ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置と、

認証センタとを備え、

ユーザ携帯装置は、原情報を分割して形成した第1情報と第2情報のうちの第1情報及び公開鍵を分割して形成した第1公開鍵と第2公開鍵のうちの第1公開鍵を記憶する第1記憶装置と、第1記憶装置に記憶されている第1情報及び第1公開鍵を送信する第1通信装置とを有し、

ユーザ装置は、原情報を分割して形成した第1情報と第2情報のうちの第2情報及び公開鍵を分割して得た第1公開鍵と第2公開鍵のうちの第2公開鍵を記憶する第2記憶装置と、第2通信装置と、第2通信装置で受信した第1情報と第2記憶手段に記憶している第2情報を、第2通信装置で受信した第1公開鍵と第2記憶手段に記憶している第2公開鍵を結合して形成した公開鍵を用いて暗号化して認証センタに送信する第3通信装置とを有し、

認証センタは、ユーザ装置から送信された暗号化情報を、ユーザ装置で用いられている公開鍵に対応する秘密鍵を用いて復号化し、復号化された第1情報と第2情報を結合し、原情報を形成することができた場合に本人であることを確認する本人確認装置を有する、

ことを特徴とする本人確認装置。

28. ユーザが携帯し、原情報を分割して形成した第1情報と第2情報のうちの第1情報を記憶する第1記憶装置と、第1記憶装置に記憶されている第1情報を送信する第1通信装置を有するユーザ携帯装置と、ユーザが使用するユーザ機器に設けられ、原情報を分割して形成した第1情報と第2情報のうちの第2情報を記憶する第2記憶装置と、第2通信装置と、第2通信装置により受信した情報と第2情報を結合して原情報を形成することができた場合に本人であることを確認する本人確認装置を有するユーザ装置とにより構成される本人確認装置の生成装置であって、

処理装置と、情報書込装置と、表示装置とを備え、

処理装置は、表示装置に表示されている原情報を、表示装置に表示されている分割線に基づいて分割して第1情報及び第2情報を形成し、形成した第1情報及び第2情報を情報書込装置に出力し、

情報書込装置は、処理装置から出力された第1情報をユーザ携帯装置の第1記憶装置に書き込むとともに、処理装置から出力された第2情報をユーザ装置の第2記憶装置に書き込む、

ことを特徴とする本人確認装置の生成装置。

29. ユーザが携帯し、原情報を分割して形成した第1情報と第2情報のうちの第1情報を記憶する第1記憶装置と、第1記憶装置に記憶されている第1情報を

送信する第1通信装置を有するユーザ携帯装置と、ユーザが使用するユーザ機器に設けられ、原情報を分割して形成した第1情報と第2情報のうちの第2情報を記憶する第2記憶装置と、第2通信装置と、第2通信装置により受信した情報と第2情報を結合して原情報を形成することができた場合に本人であることを確認する本人確認装置を有するユーザ装置とにより構成される本人確認装置の生成装置であって、

処理装置と、情報書込装置と、入力装置とを備え、

処理装置は、入力装置より入力された原情報を、入力装置により指示された分割方法で分割して第1情報と第2情報を形成し、形成した第1情報及び第2情報を情報書込装置に出力し、

情報書込装置は、処理装置から出力された第1情報をユーザ携帯装置の第1記憶装置に書き込むとともに、処理装置から出力された第2情報をユーザ装置の第2記憶装置に書き込む、

ことを特徴とする本人確認装置の生成装置。

30. 請求項29に記載の本人確認装置の生成装置であって、

更に、商品排出装置を備え、

商品排出装置は、情報書込装置によって第1情報が書き込まれたユーザ携帯装置及び第2情報が書き込まれたユーザ装置を商品排出口から排出する、

ことを特徴とする本人確認装置の生成装置。

31. 第1情報を送信する第1の装置と、第1の装置から受信した第1の情報と自身が記憶している第2の情報を結合し、所定の情報を形成することができた場合に本人であることを確認する本人確認装置の生成方法であって、

暗号化式及び復号化式を生成し、暗号化式を用いて暗号化を行い、復号化式を用いて復号化を行う暗号装置と、暗号装置によって生成された暗号化式を用いて原コードを暗号化した暗号化コードを記憶する暗号化コード記憶装置と、暗号装置によって生成された復号化式と原コードを記憶する原コード記憶装置を有する回路基板を用意するステップと、

回路基板を切断して、暗号装置と原コード記憶装置を有する第1回路基板と、暗号化コード記憶装置を有する第2回路基板を形成するステップと、

第1回路基板を第2の装置に用い、第2回路基板を第1の装置に用いるステップと、

を備えることを特徴とする本人確認装置の生成方法。

32. 請求項31に記載の本人確認装置の生成方法であって、

暗号装置は、時間的に変化する暗号化式及び復号化式を生成するものであり、

暗号化コード記憶装置には、回路基板切断時の暗号化式を用いて原コードを暗号化した暗号化コードが記憶保持され、

原コード記憶装置には、回路基板切断時の復号化式と原コードが記憶されている、

ことを特徴とする本人確認装置の生成方法。

33. 請求項32に記載の本人確認装置の生成方法であって、

暗号装置は、カオスジェネレータで生成されたカオス演算式を用いて暗号化及び復号化を行う、

ことを特徴とする本人確認装置の生成方法。

34. 請求項31に記載の本人確認装置の生成方法であって、回路基板を切断するステップでは、回路基板に形成されている切断部の個所を切断する、ことを特徴とする本人確認装置の生成方法。

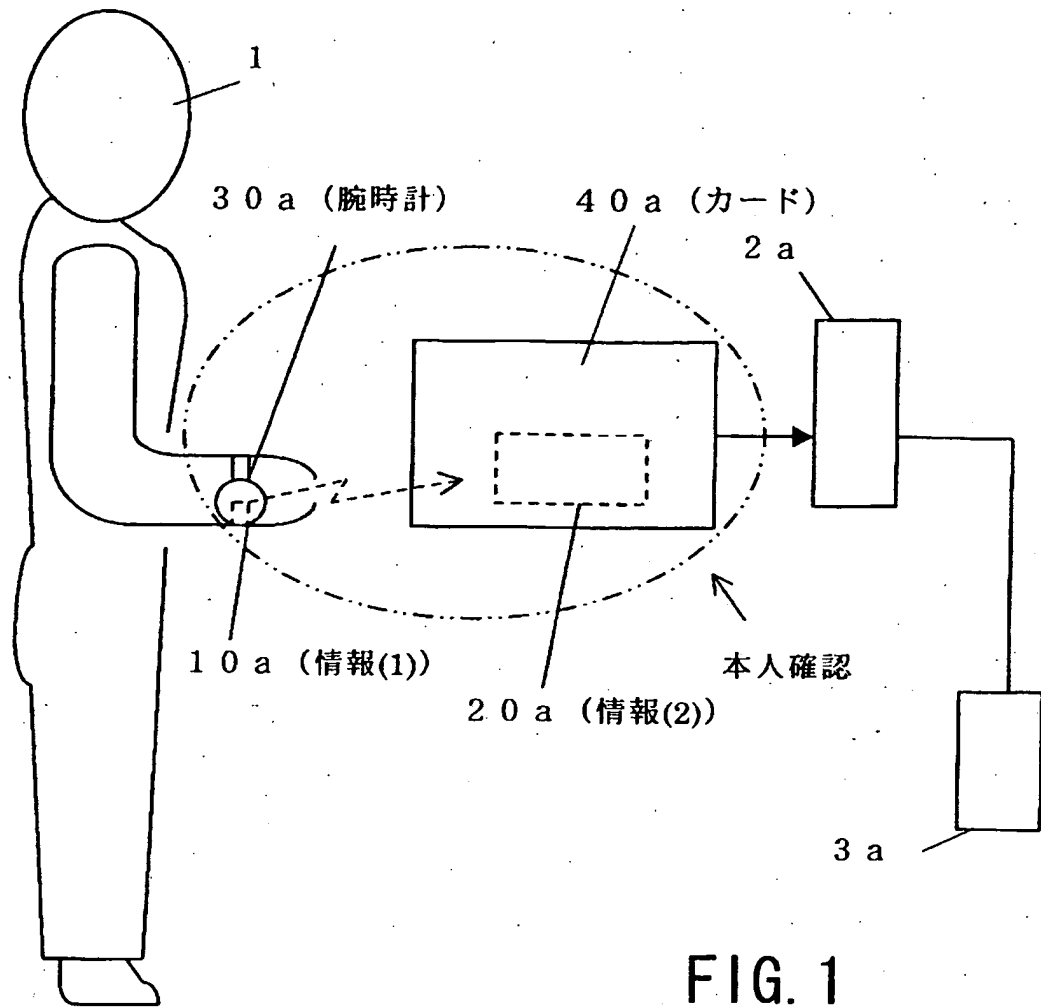


FIG. 1

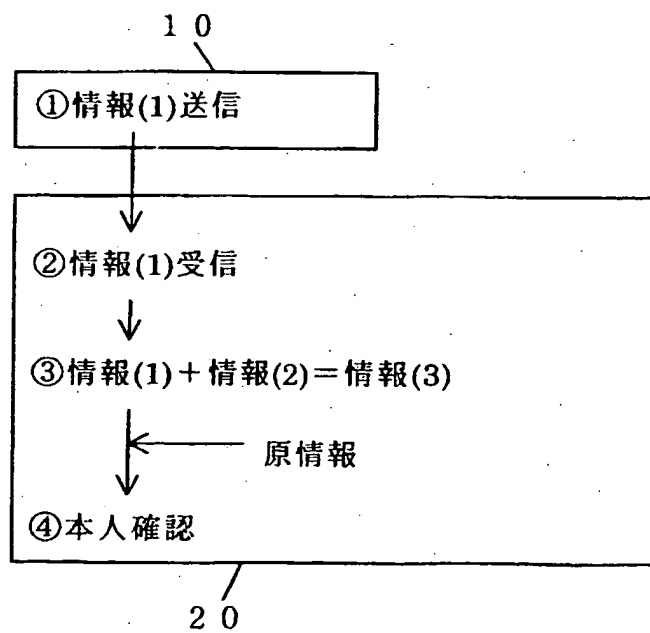


FIG. 2

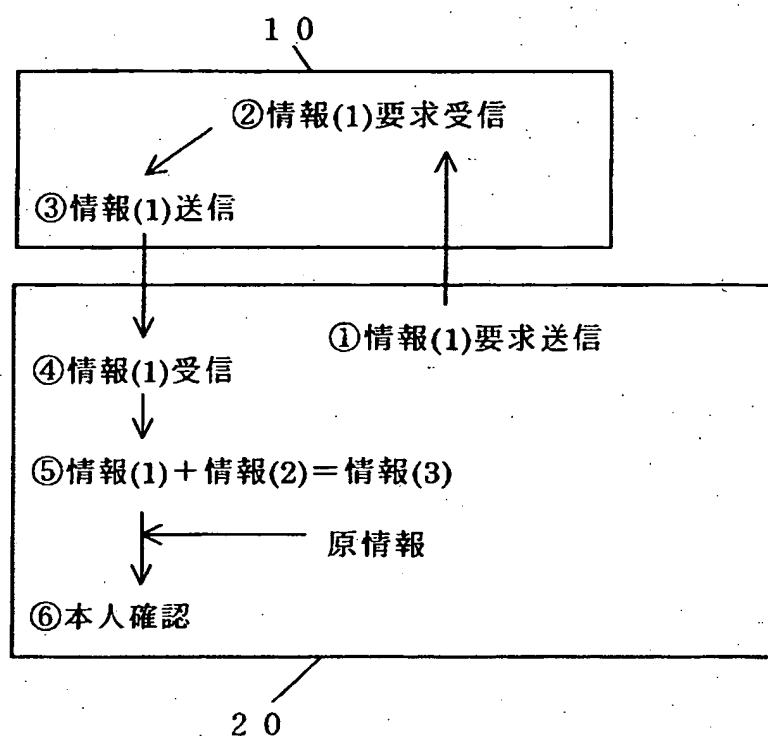


FIG. 3

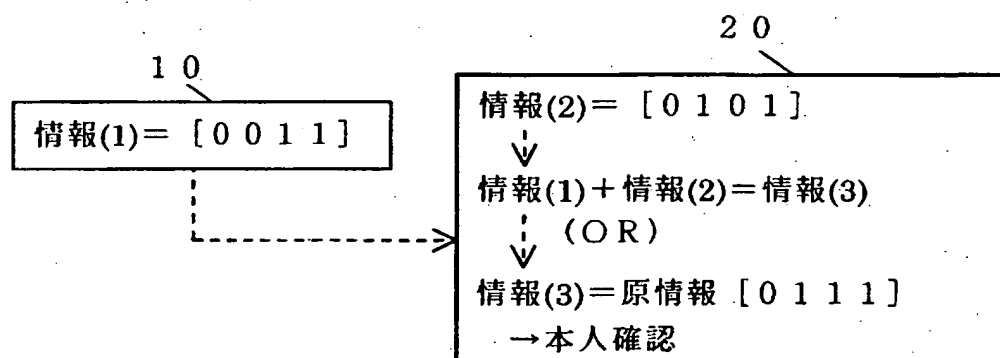


FIG. 4

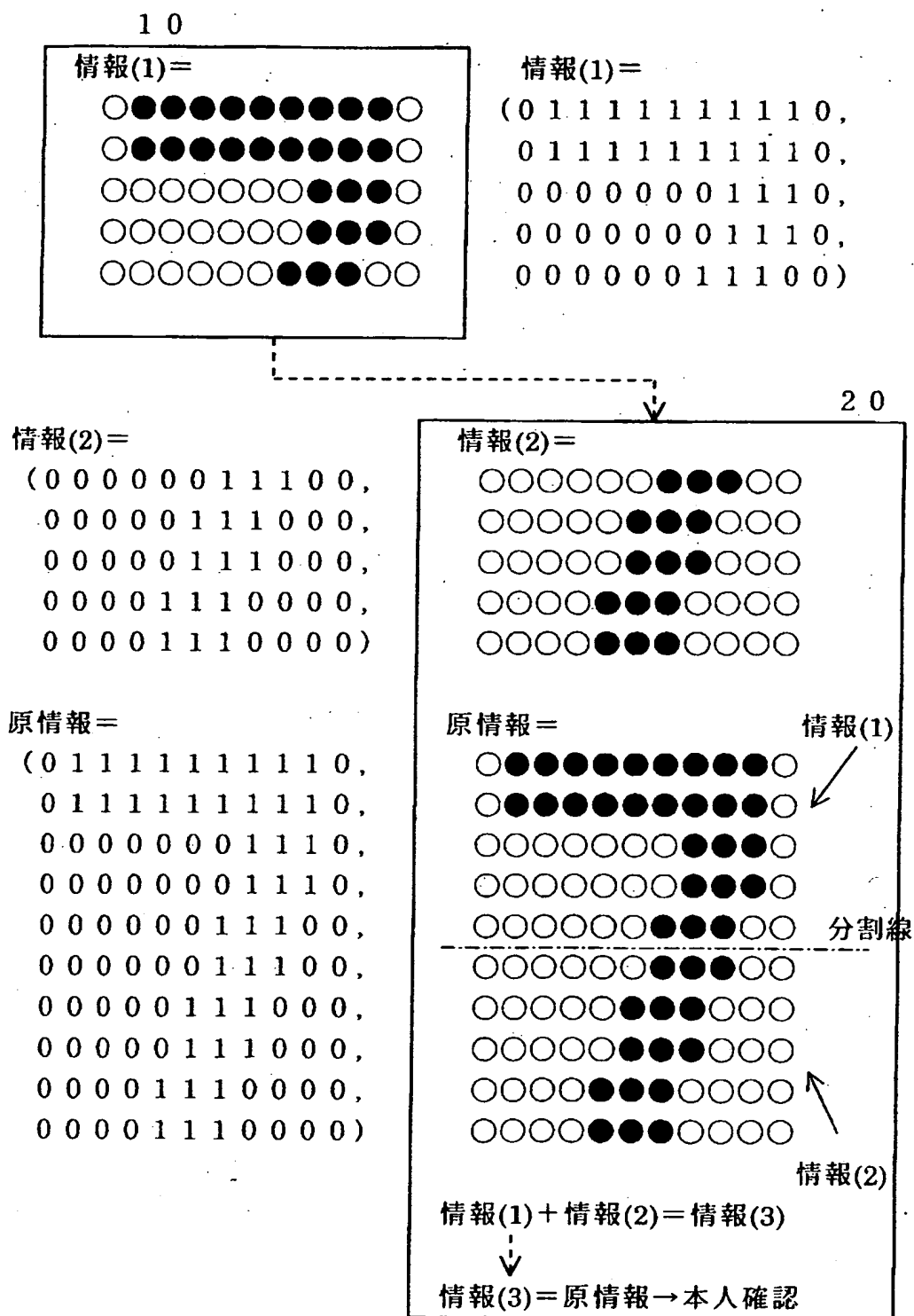


FIG. 5

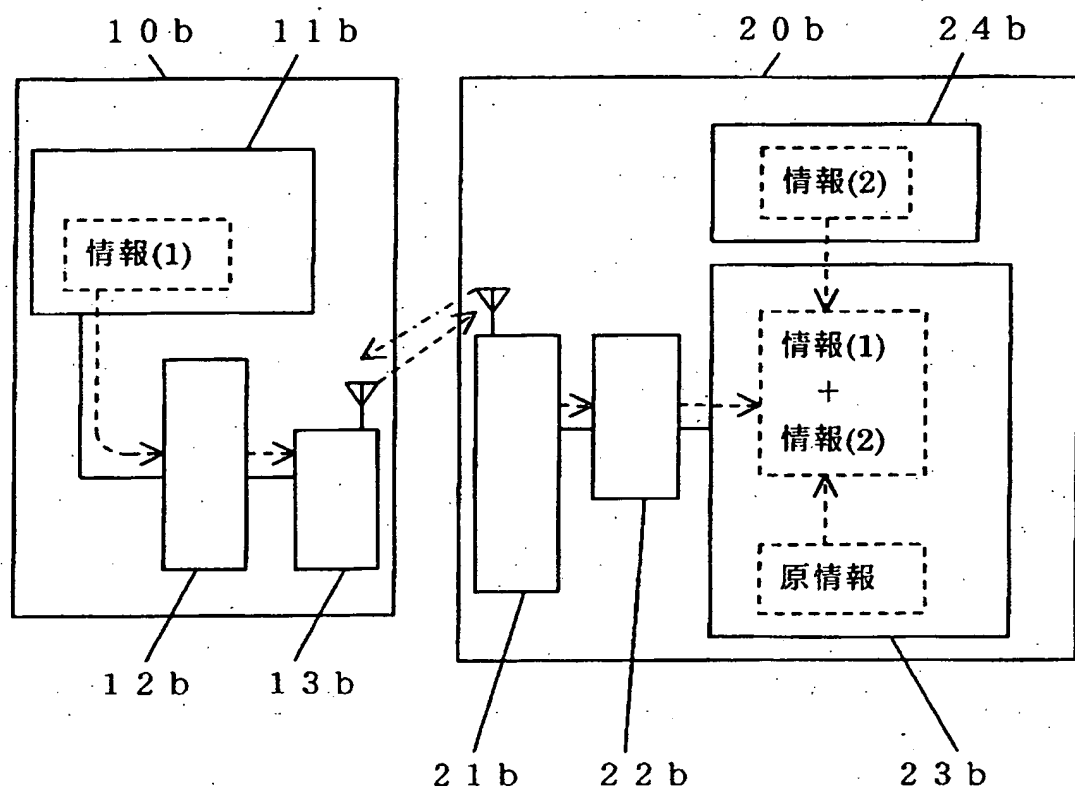


FIG. 6

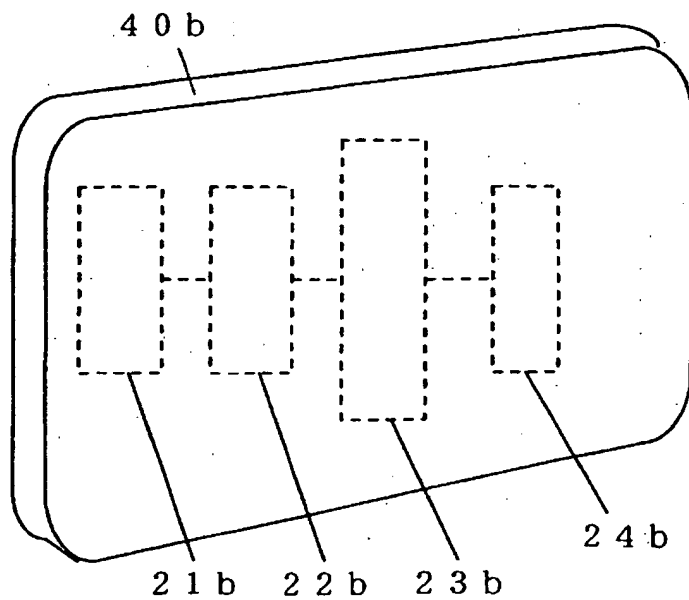


FIG. 7

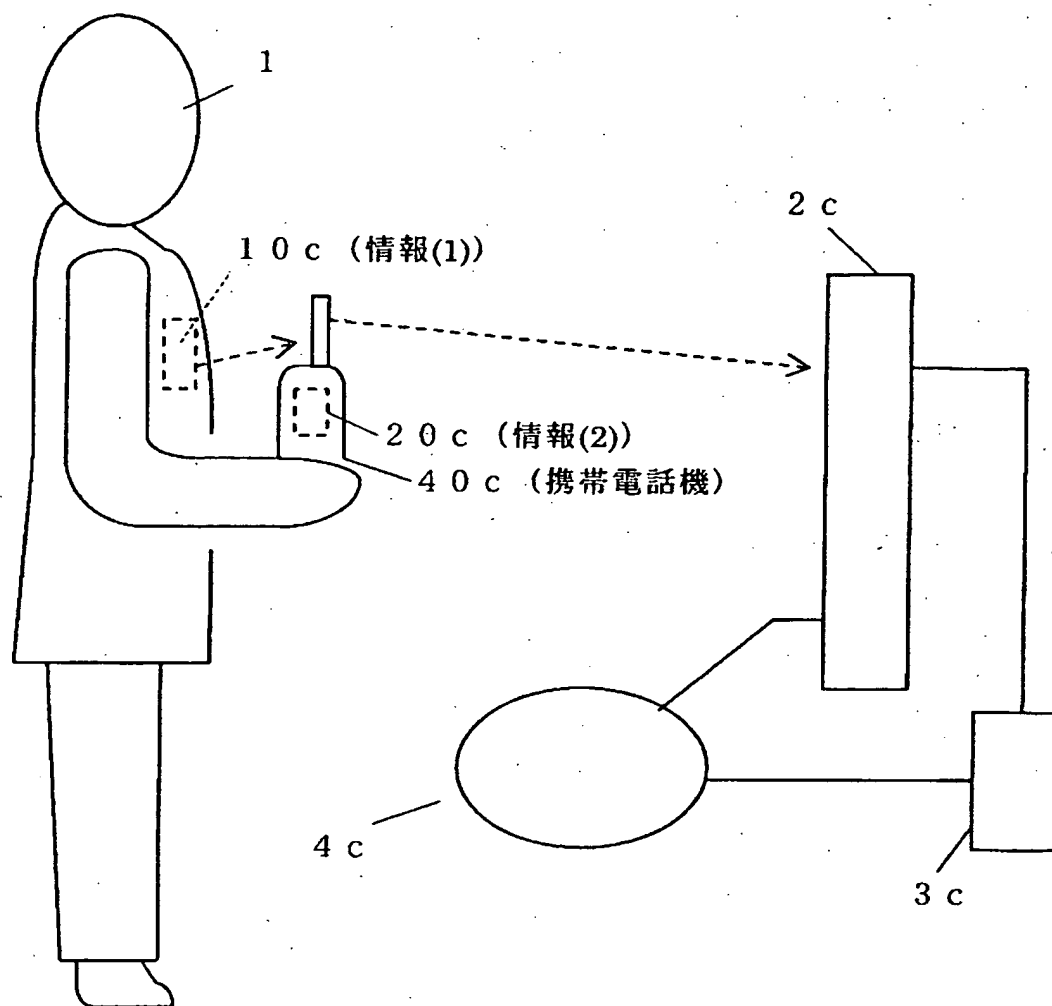


FIG. 8

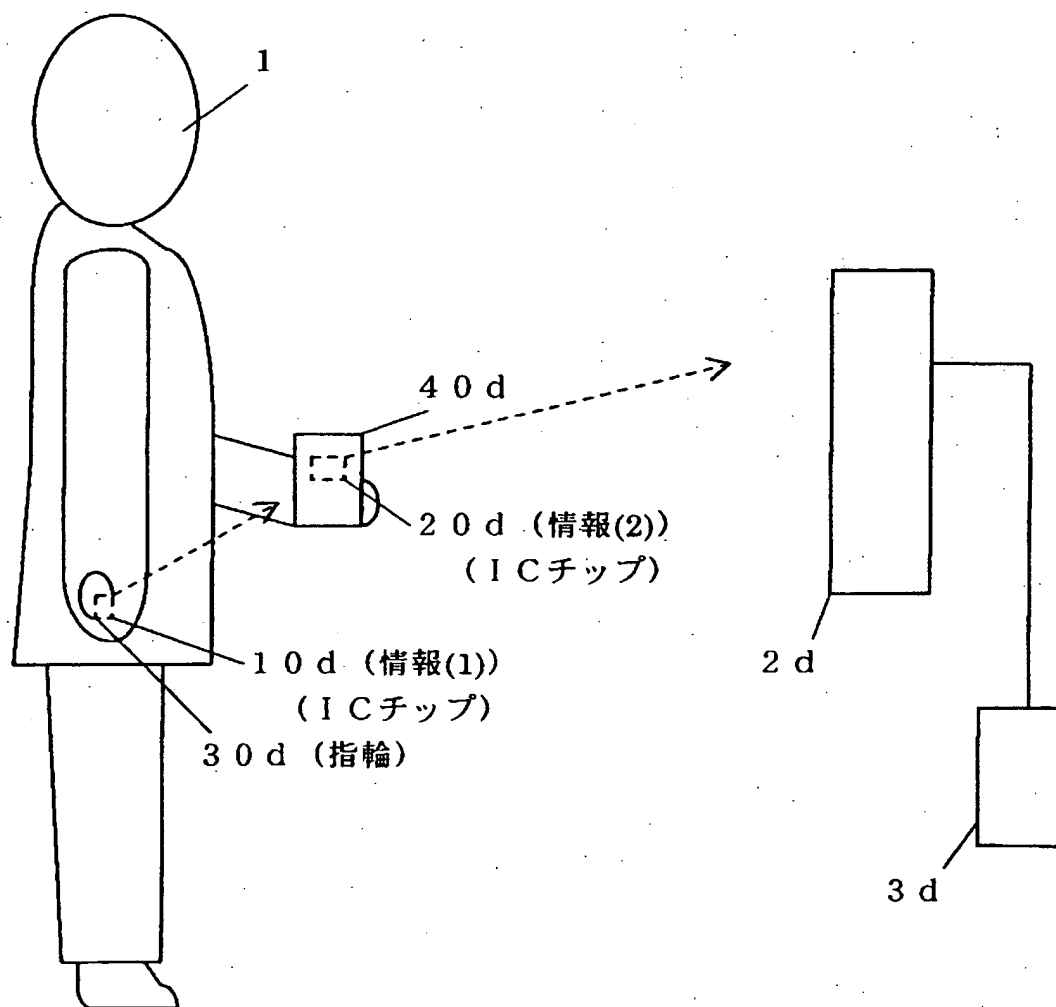


FIG. 9

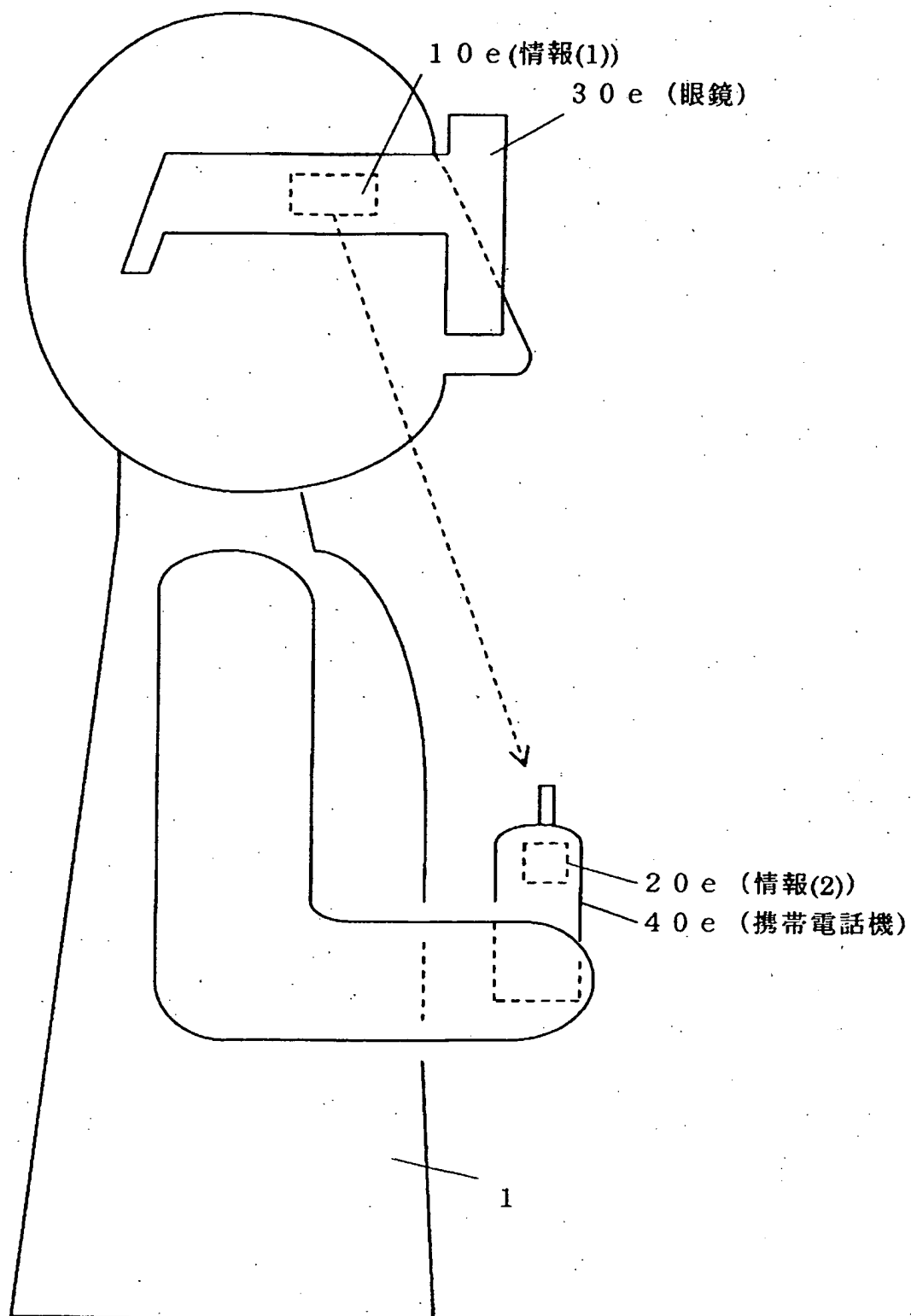


FIG. 10

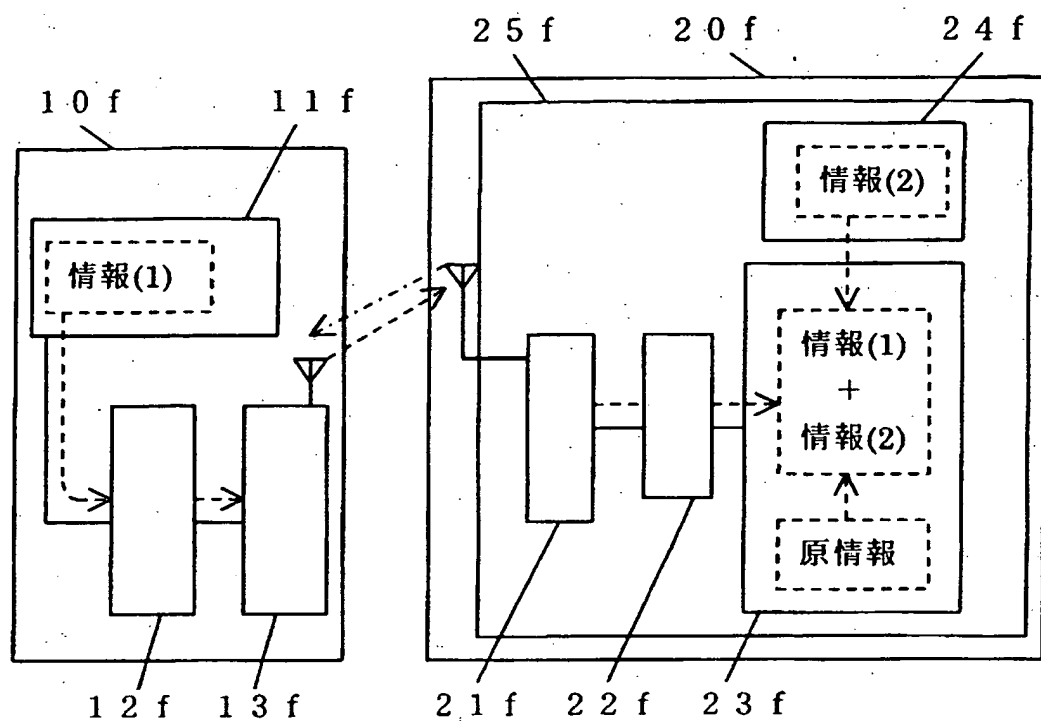


FIG. 11

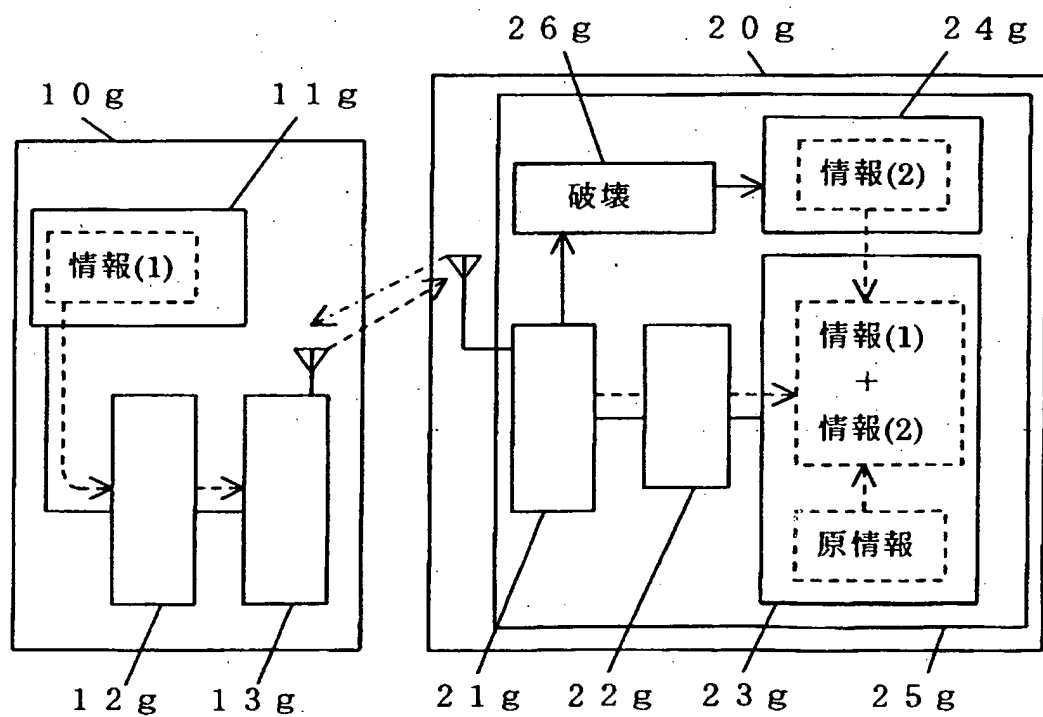


FIG. 12

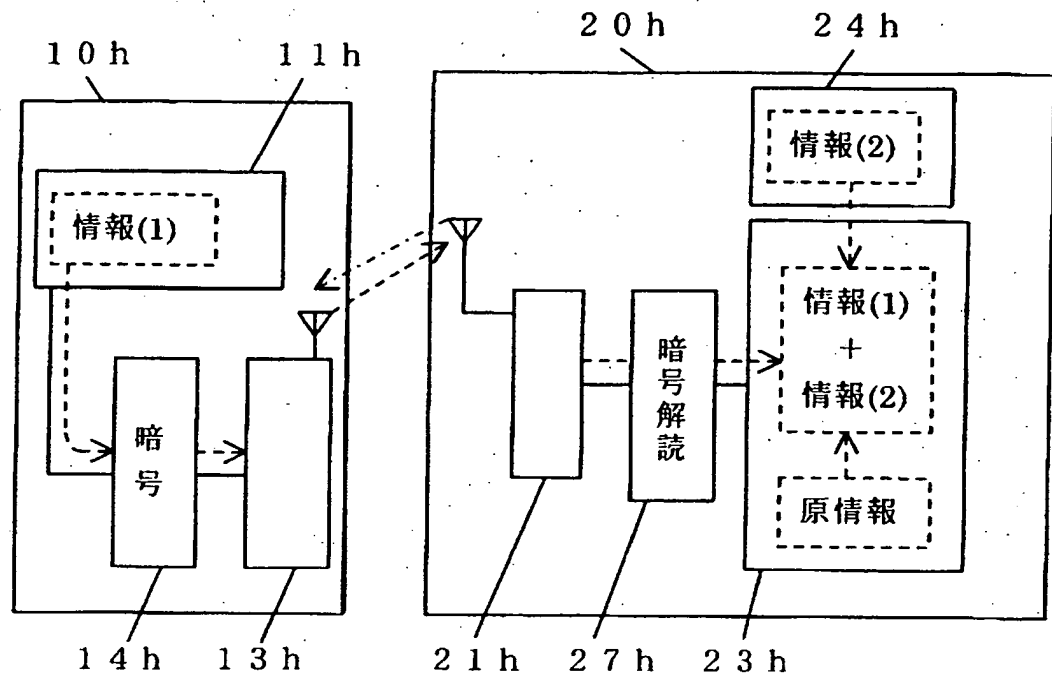


FIG. 13

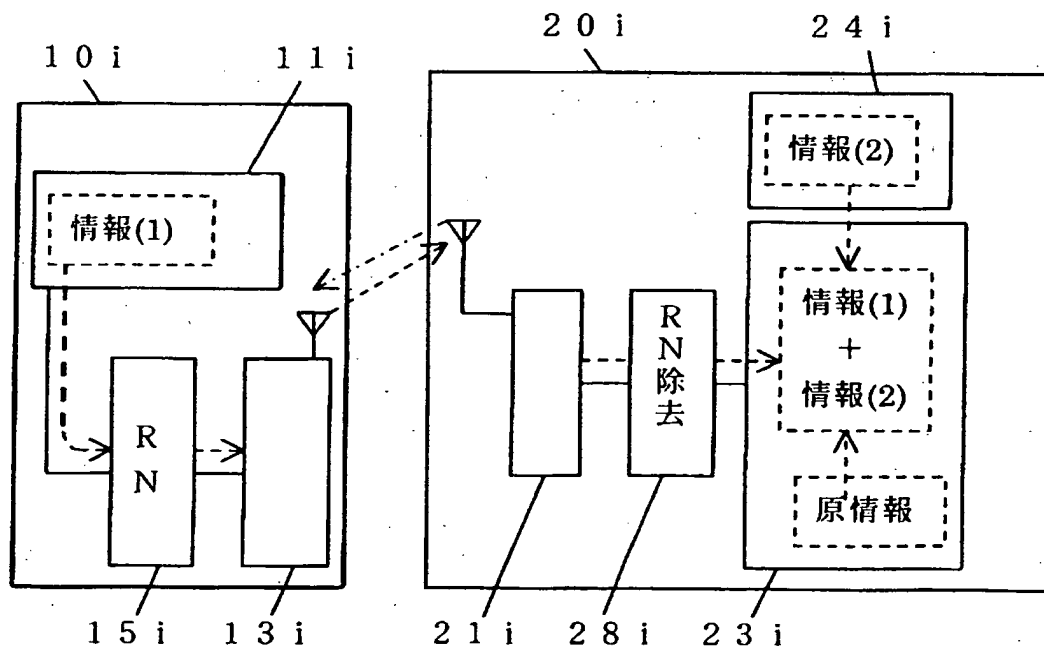


FIG. 14

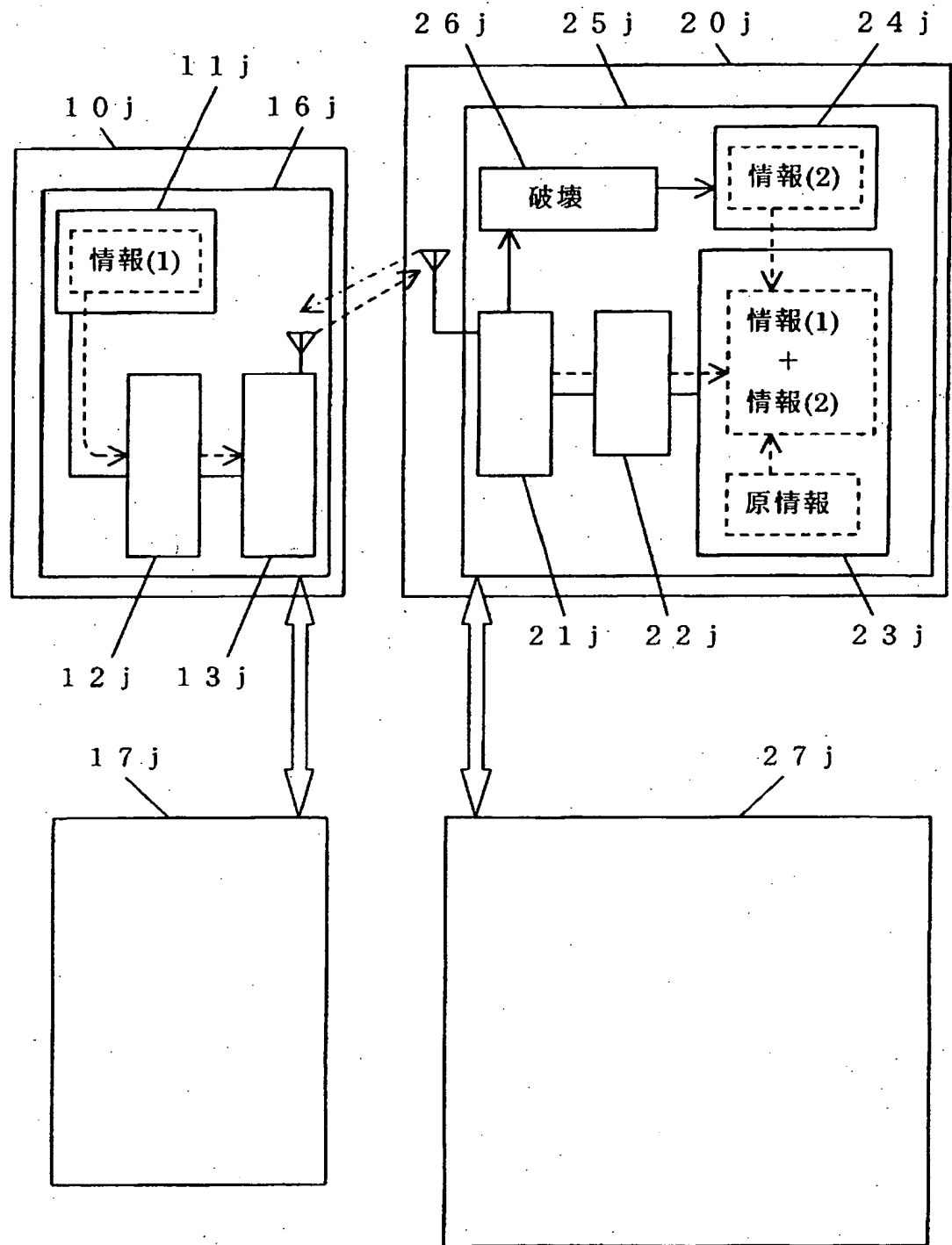


FIG. 15

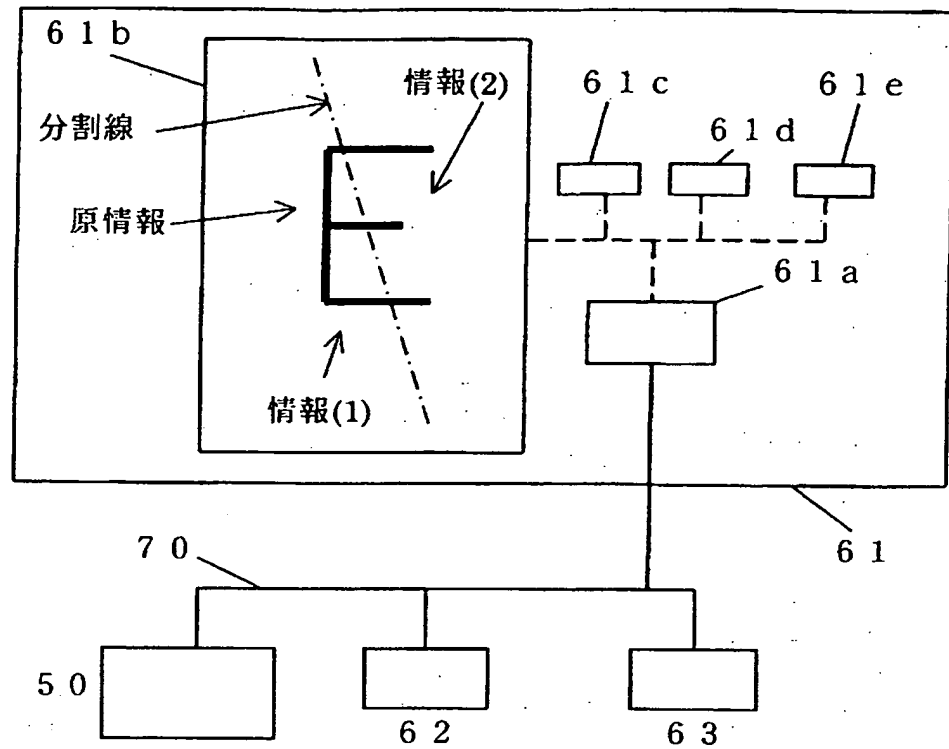


FIG. 16

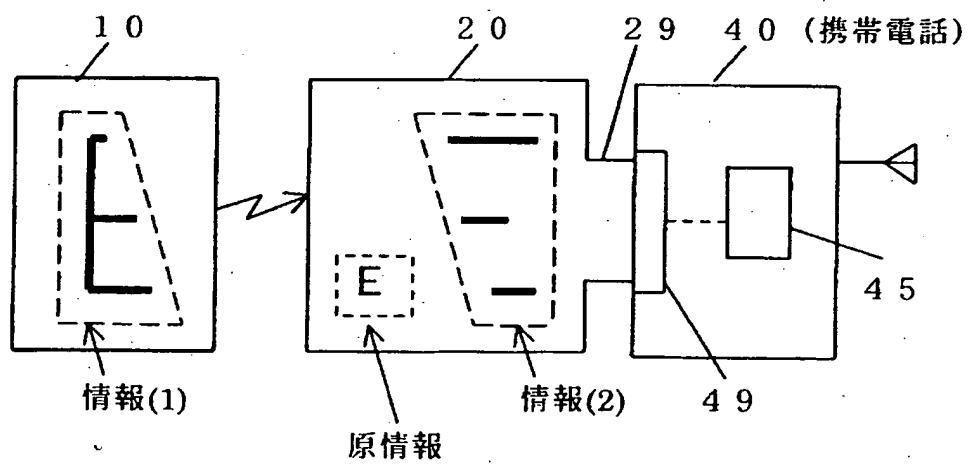


FIG. 17

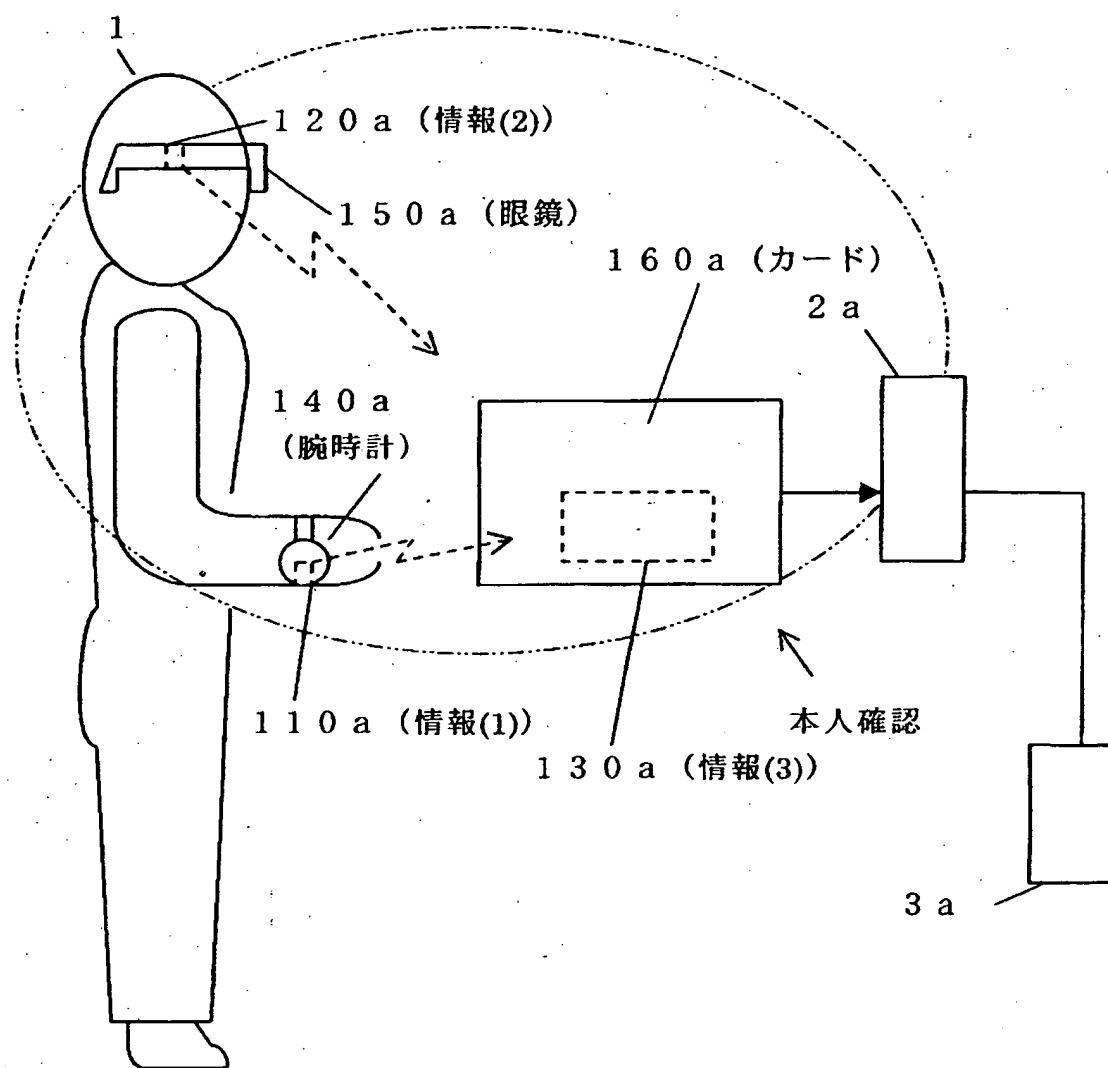


FIG. 18

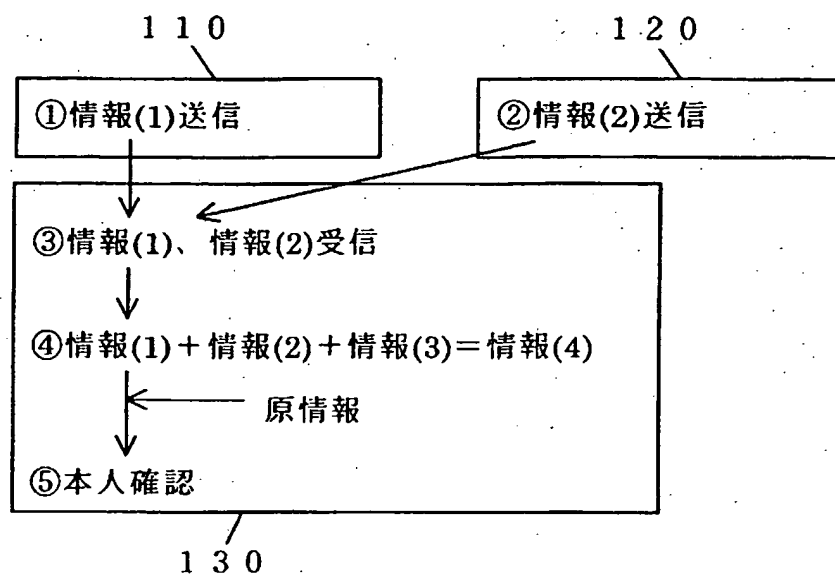


FIG. 19

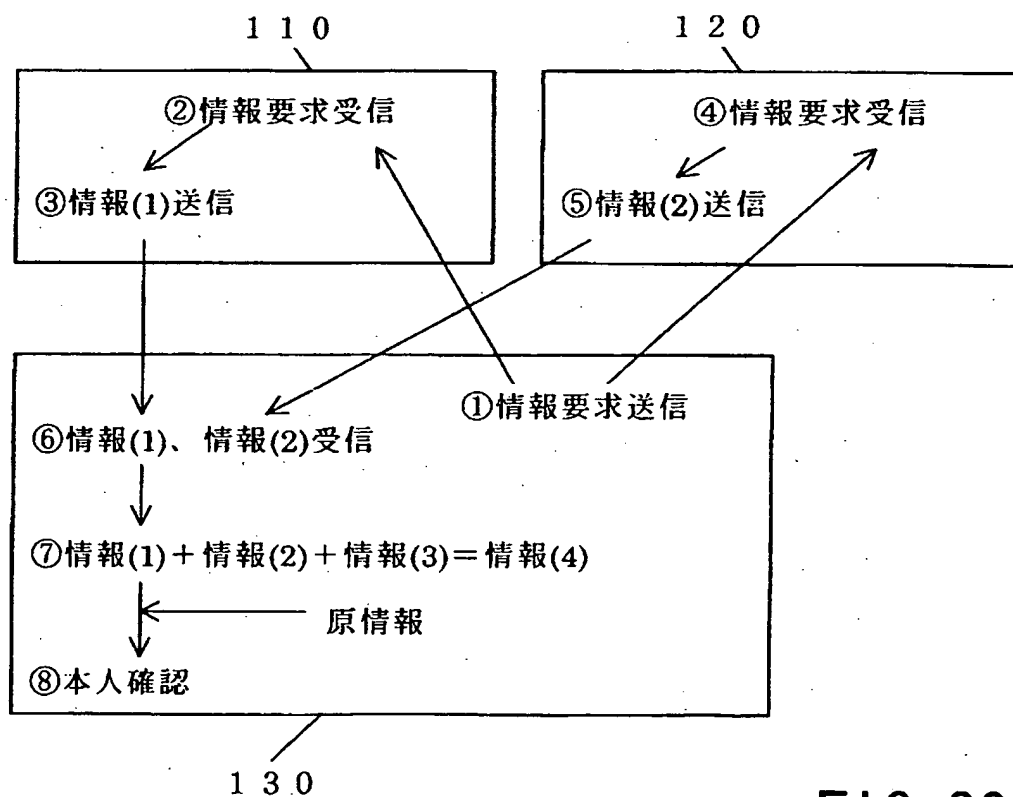


FIG. 20

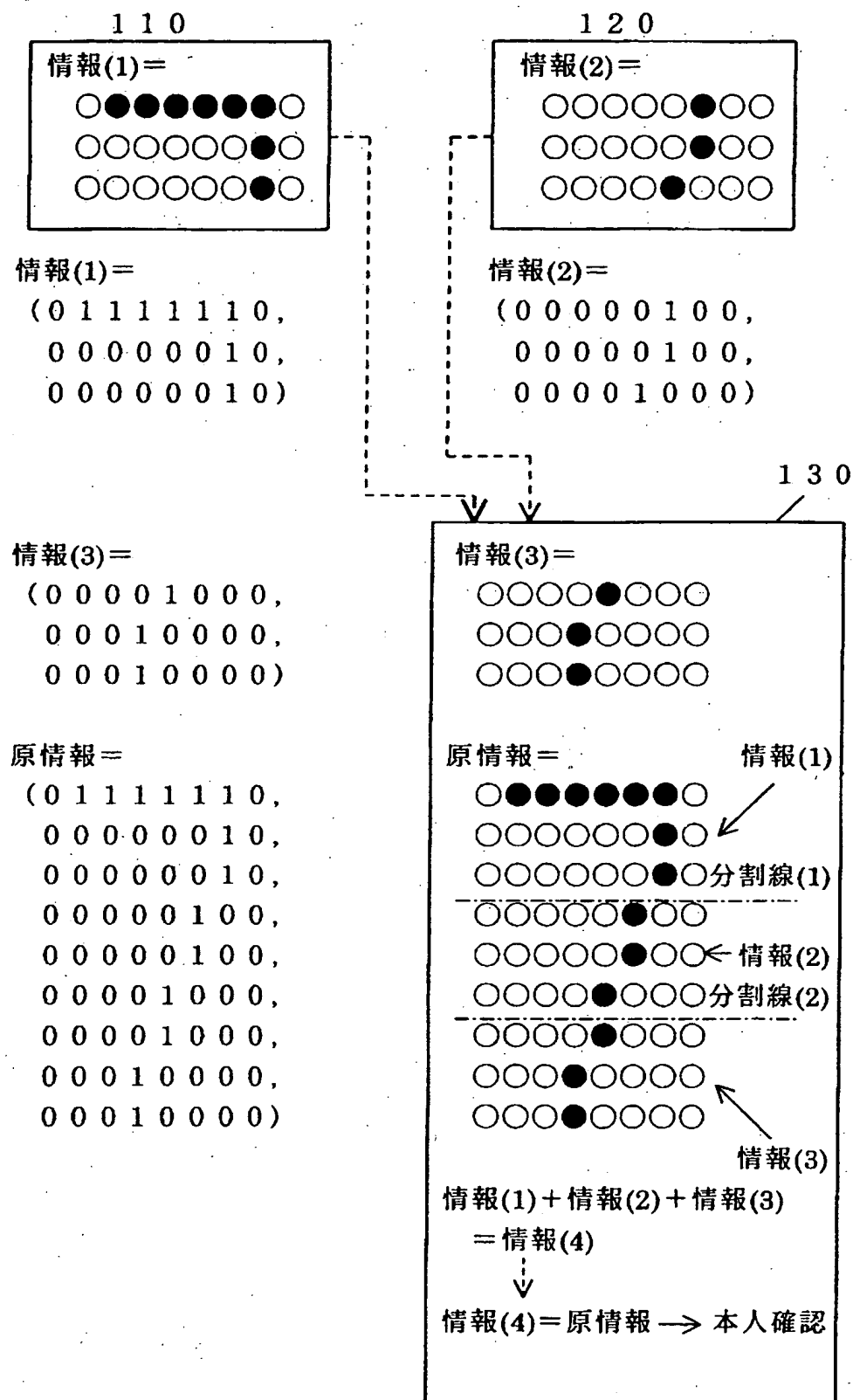


FIG. 21

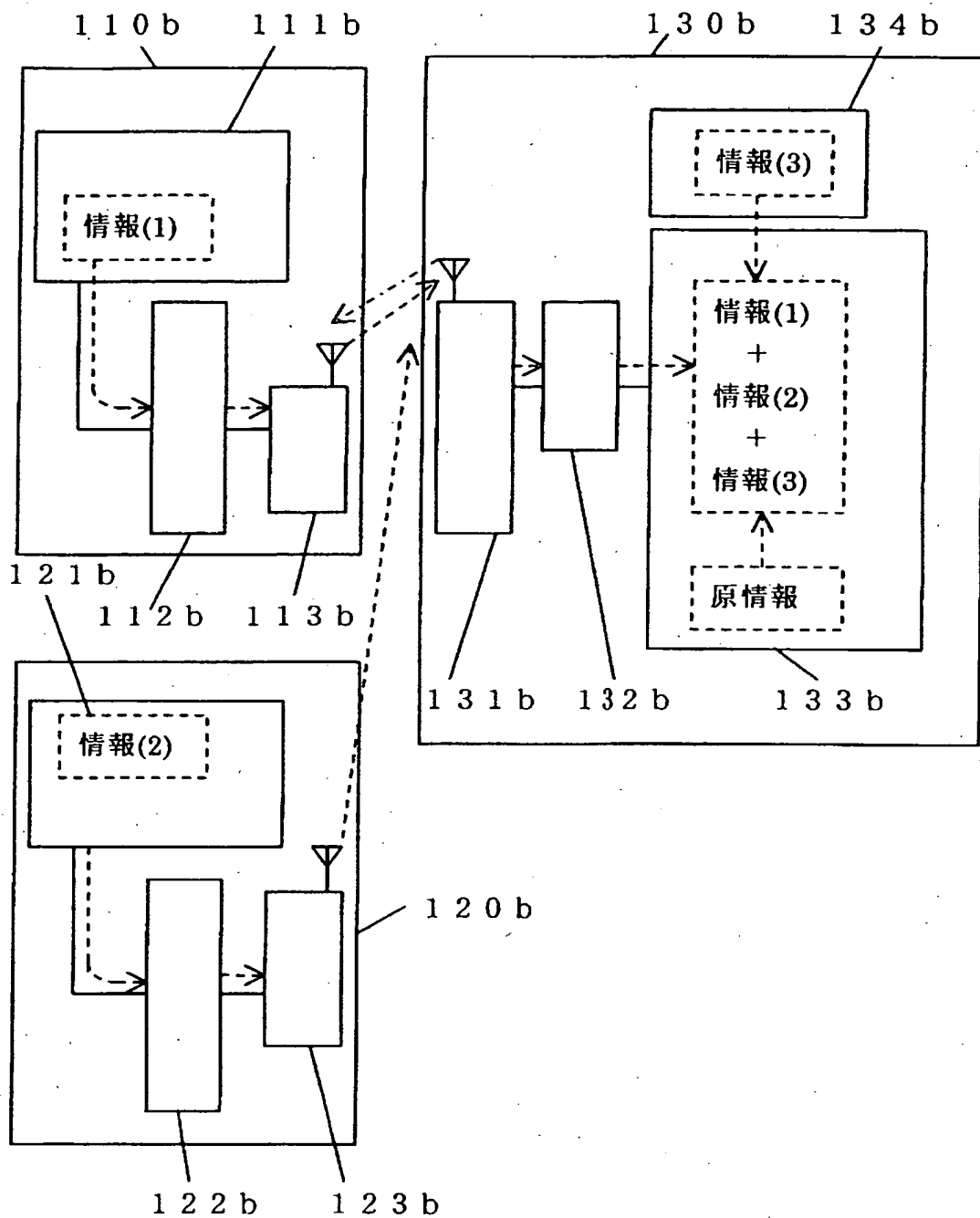


FIG. 22

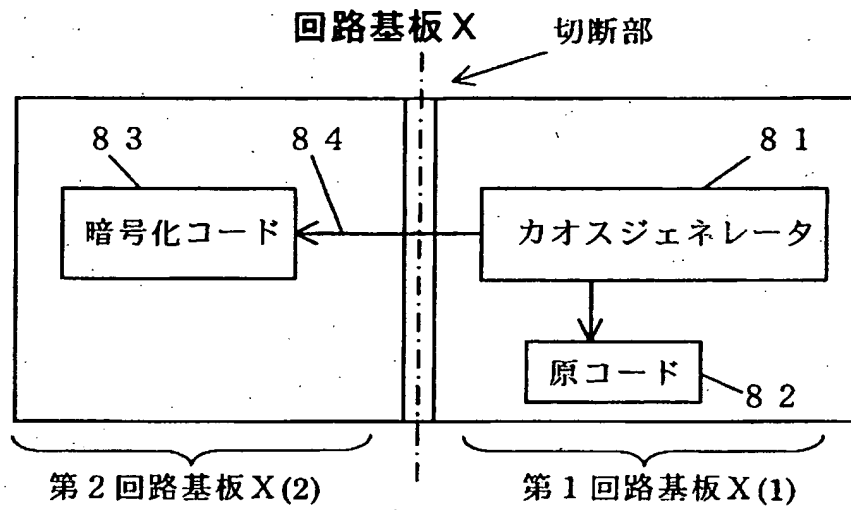


FIG. 23

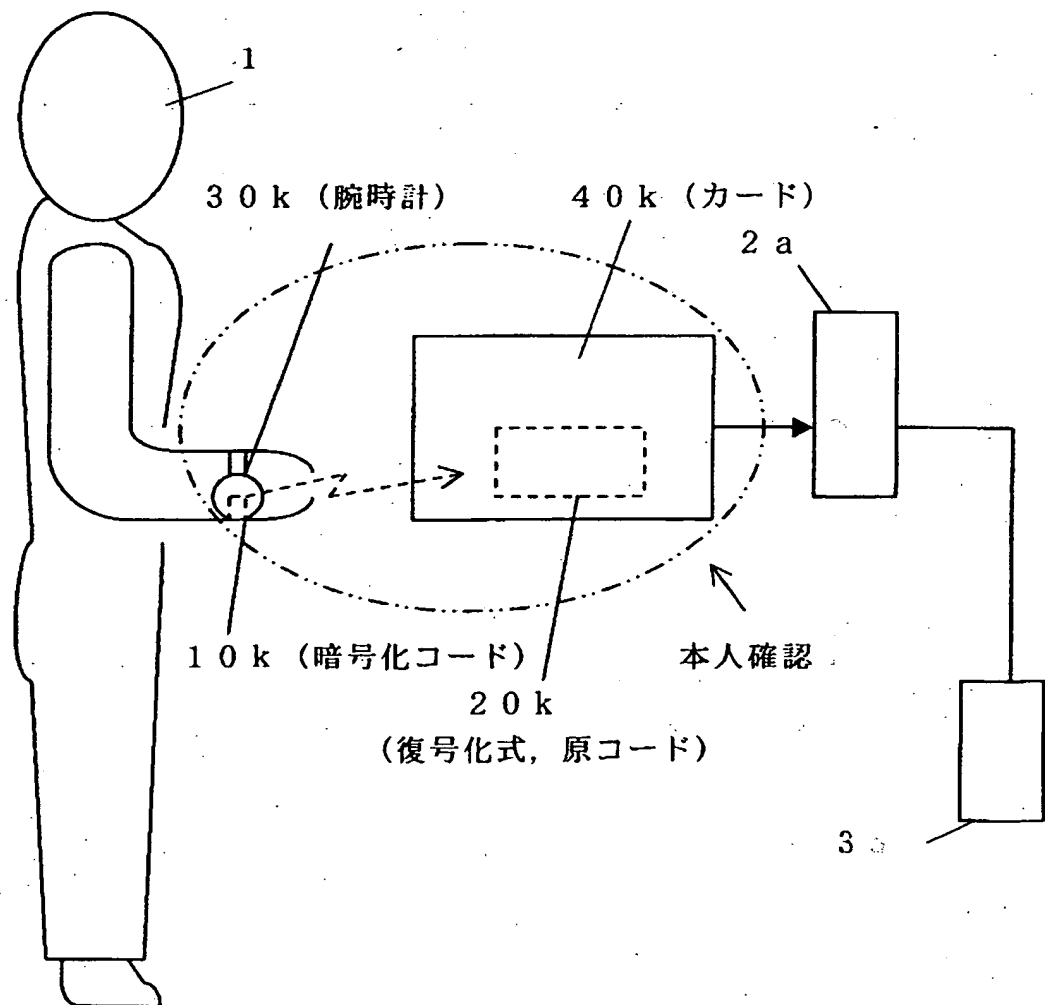


FIG. 24

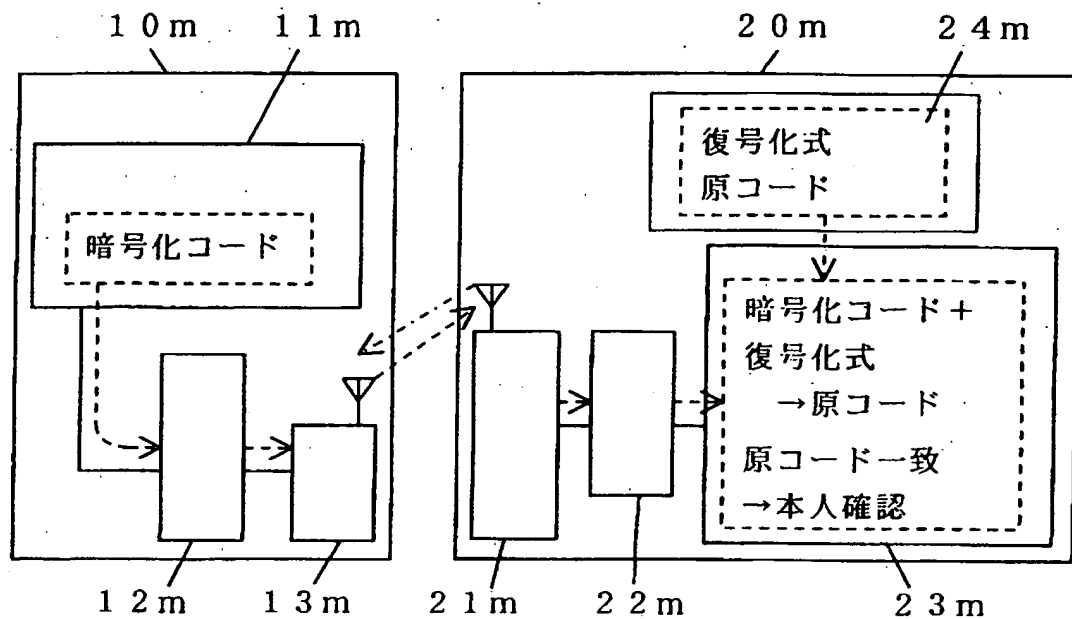


FIG. 25

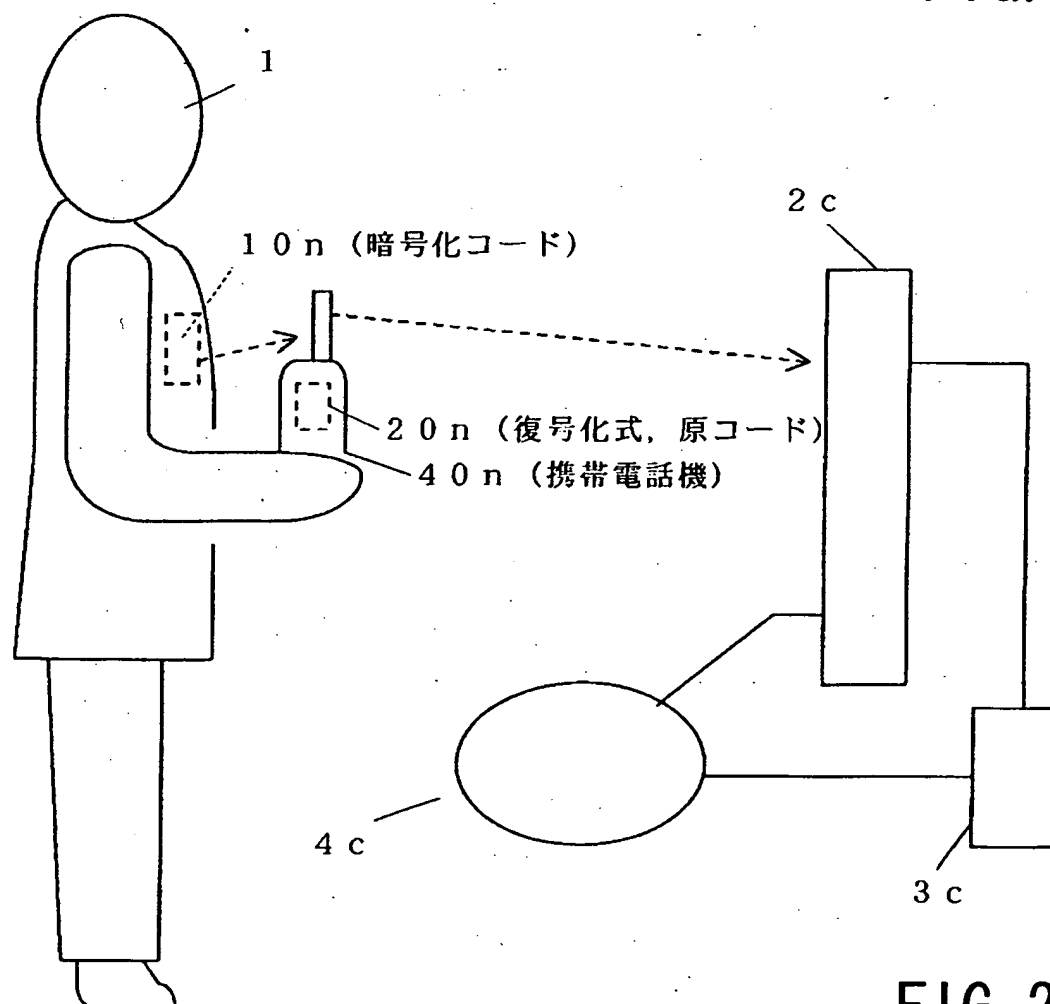


FIG. 26

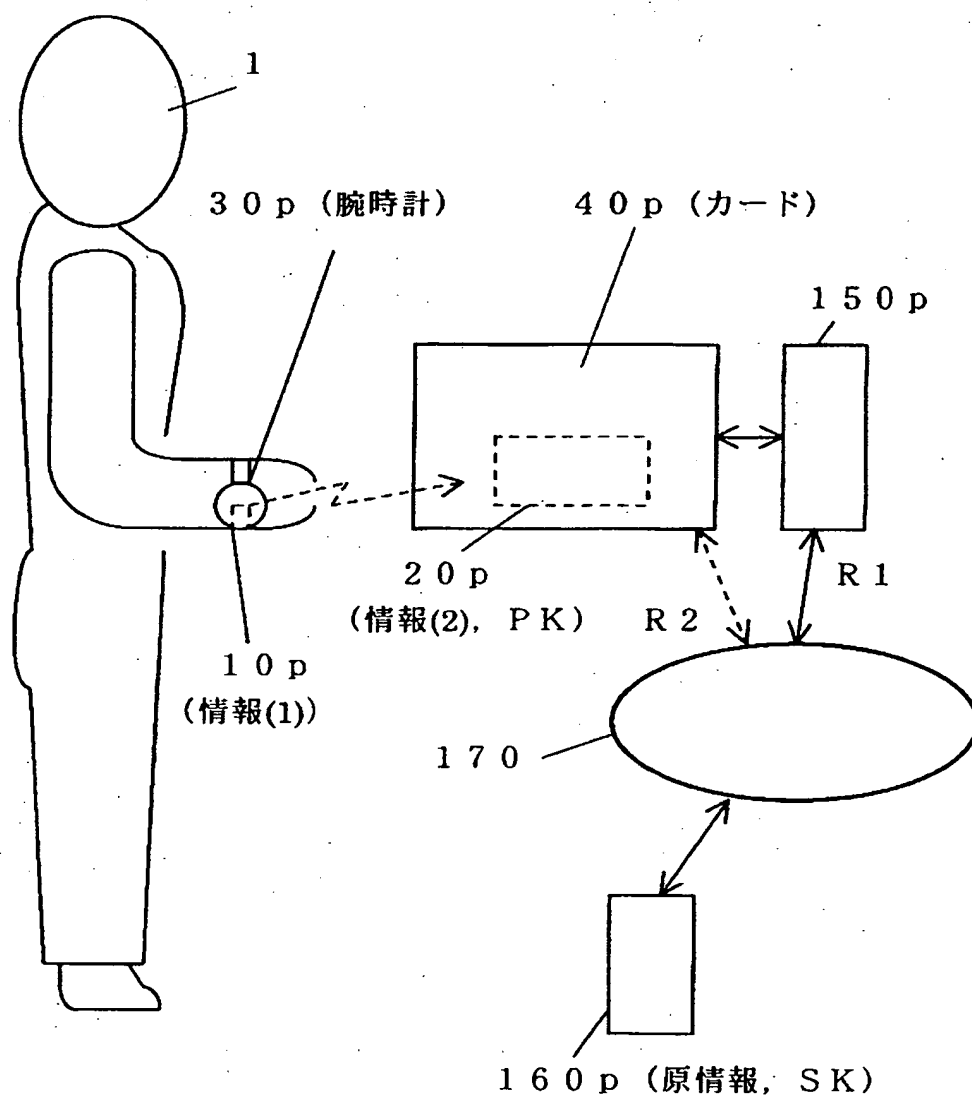


FIG. 27

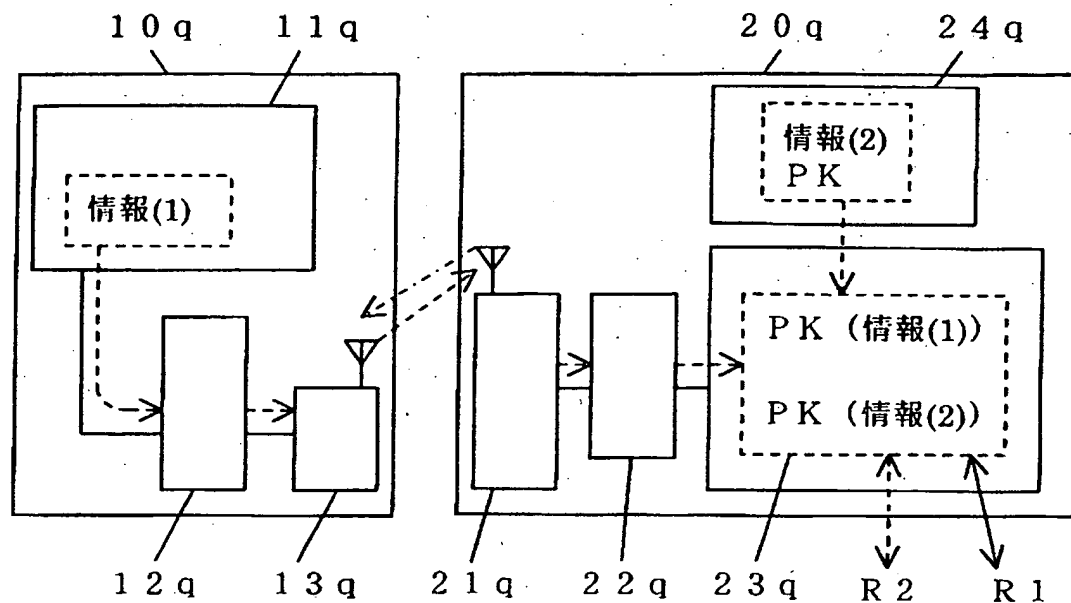


FIG. 28

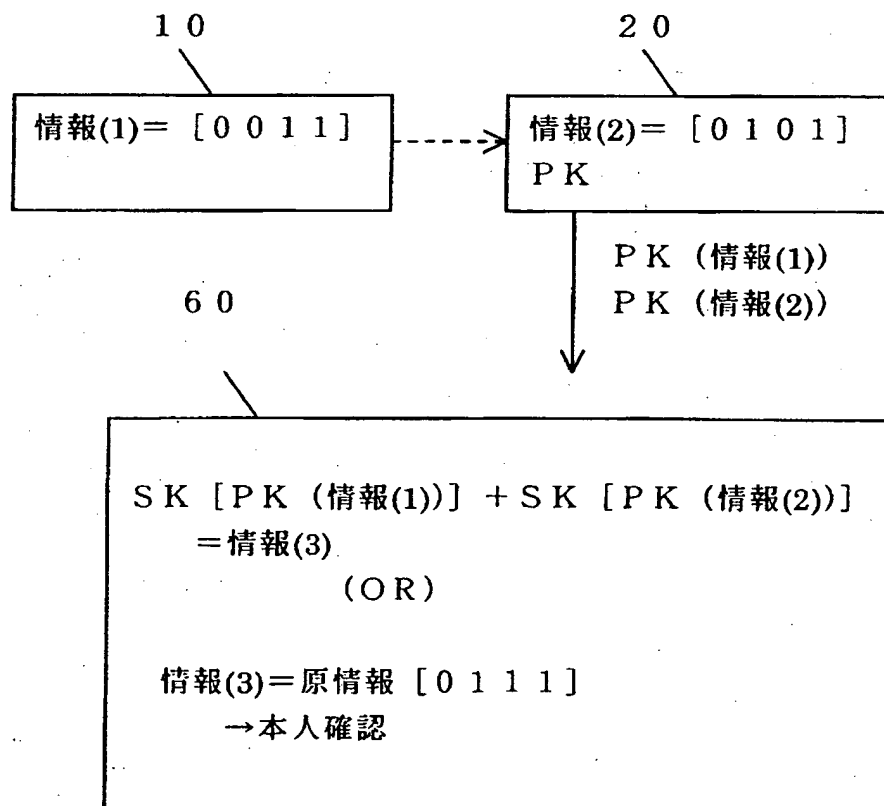


FIG. 29

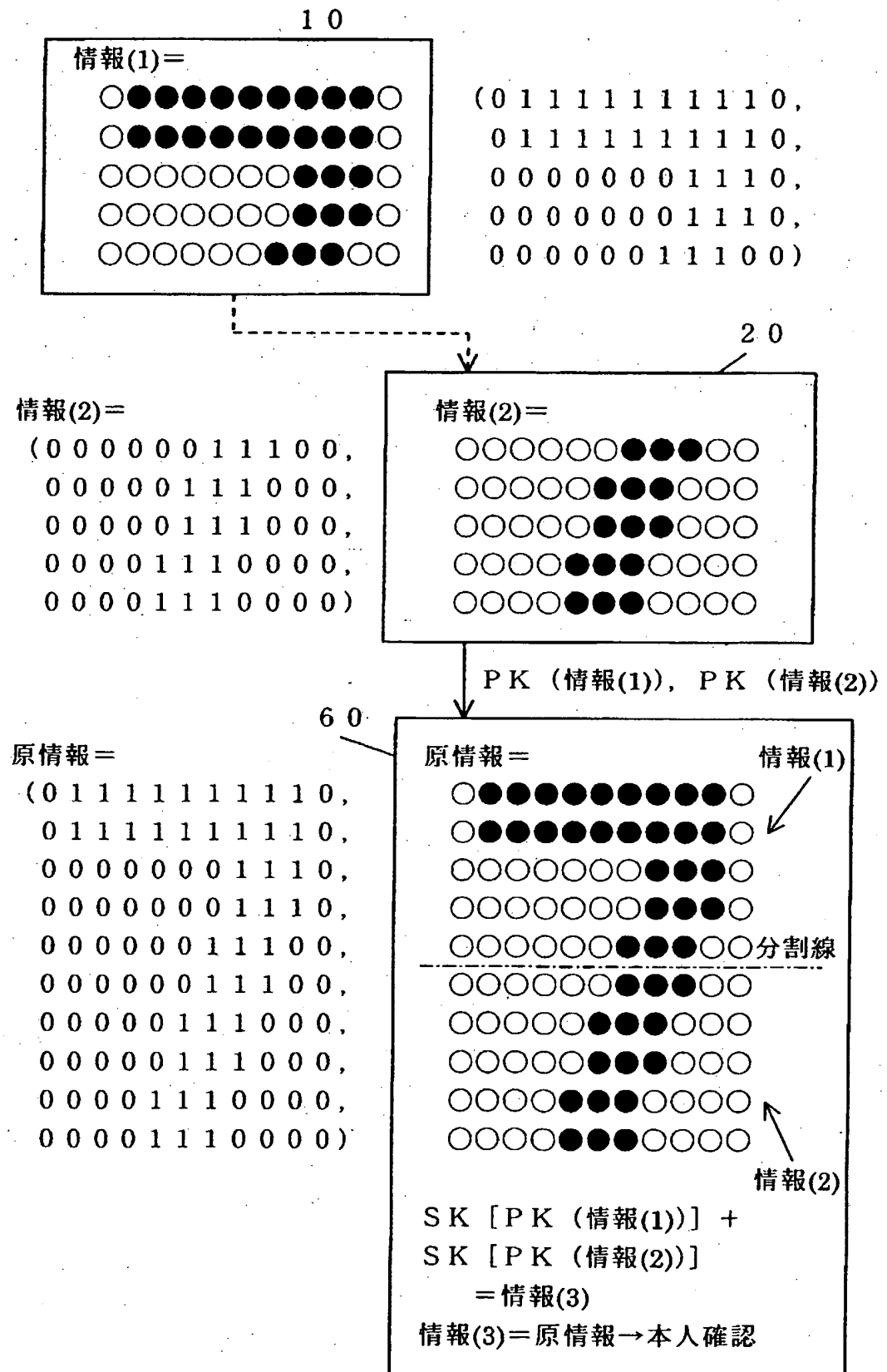


FIG. 30

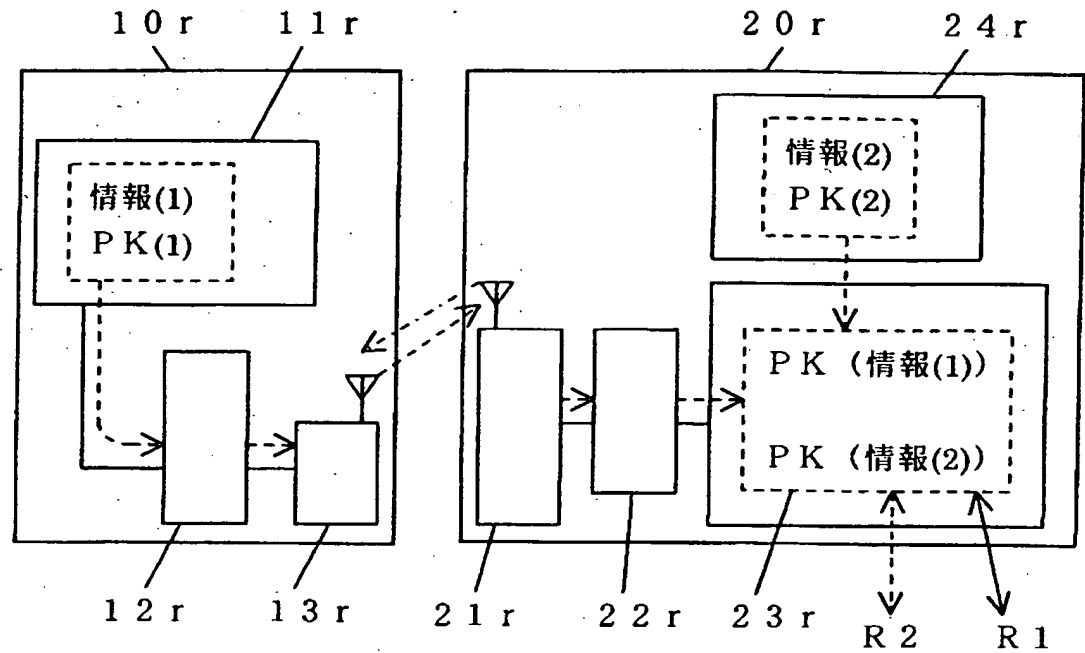


FIG. 31

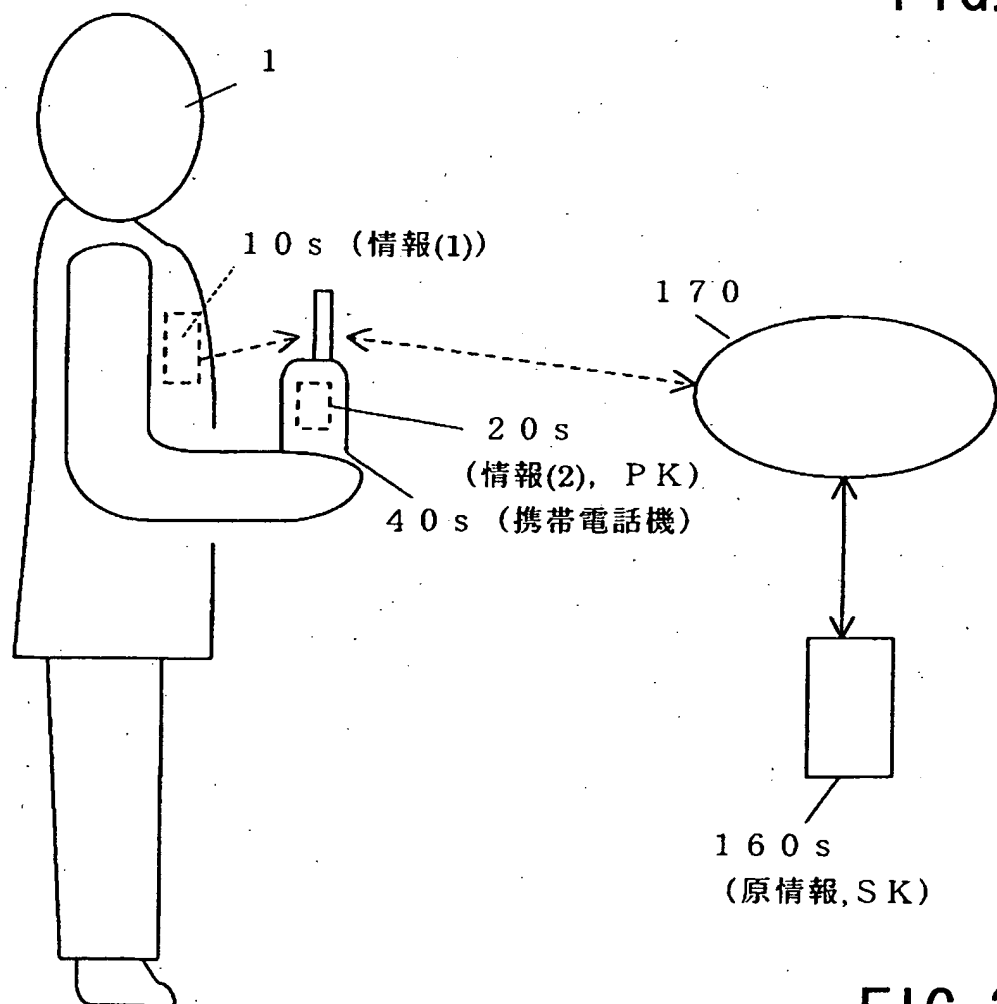


FIG. 32

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02329

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, G06F17/60, G06K17/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP, 04-306760, A (Nippon Telegr. & Teleph. Corp. <NTT>), 29 October, 1992 (29.10.92) (Family: none) Full text	1-27 28-34
Y A	JP, 10-149339, A (Mitsubishi Electric Corporation), 02 June, 1998 (02.06.98) (Family: none) Claims	1-27 28-34
Y	JP, 11-167664, A (Nippon Conlux Co., Ltd.), 22 June, 1999 (22.06.99) (Family: none) Claim 6	3,10
Y	JP, 2000-11129, A (Nippon Telegr. & Teleph. Corp. <NTT>), 14 January, 2000 (14.01.00) (Family: none) description; Par. Nos. [0002] to [0004]	11,12
Y	JP, 10-322325, A (Shusuke YAMAJI), 04 December, 1998 (04.12.98) (Family: none) Claims	23,27

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
13 June, 2001 (13.06.01)

Date of mailing of the international search report
26 June, 2001 (26.06.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02329

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 62-191198, A (Tokyo Tatsuno Co., Ltd.), 21 August, 1987 (21.08.87) (Family: none) Full text	31-34
A	JP, 04-335730, A (Toshiba Corporation), 24 November, 1992 (24.11.92) (Family: none) Claims	31-34

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. G06F15/00, G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. G06F15/00, G06F17/60, G06K17/00, H04L9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2001年
 日本国実用新案登録公報 1996-2001年
 日本国登録実用新案公報 1994-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	JP, 04-306760, A (日本電信電話株式会社), 29. 10月. 1992 (29. 10. 92) (ファミリーなし) 全文	1-27 28-34
Y A	JP, 10-149339, A (三菱電機株式会社), 2. 6月. 1998 (02. 06. 98) (ファミリーなし) 特許請求の範囲	1-27 28-34
Y	JP, 11-167664, A (株式会社日本コンラックス), 2 2. 6月. 1999年 (22. 06. 99) (ファミリーなし) 請求項6	3, 10

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

13. 06. 01

国際調査報告の発送日

26.06.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

宮司 卓佳



5B

9555

電話番号 03-3581-1101 内線 3545

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 2000-11129, A (日本電信電話株式会社), 14. 1月. 2000 (14. 01. 00) (ファミリーなし) 明細書第2段落~同第4段落	11, 12
Y	J P, 10-322325, A (山地秀典), 4. 12月. 199 8 (04. 12. 98) (ファミリーなし) 特許請求の範囲	23, 27
A	J P, 62-191198, A (株式会社東京タツノ), 21. 8 月. 1987 (21. 08. 87) (ファミリーなし) 全文	31-34
A	J P, 04-335730, A (株式会社東芝), 24. 11月. 1992 (24. 11. 92) (ファミリーなし) 特許請求の範囲	31-34